A Lightweight Symmetric Cryptography based User Authentication Protocol for IoT based Aquaculture Monitoring System

Alumuru.Mahesh Reddy[1], Machiraju.Kameswara Rao[2]

[1]Research scholar, [2]Associate Professor
Department of ECM, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, India.

Abstract

IoT is being used in a variety of settings; including tele-care, intelligent home and transportation systems. IoT device data is stored on remote servers, and access to the data requires external users to authenticate with the server. To ensure the long-term health of the network in IoT environments, the authentication procedure must be quick, secure against a variety of attacks, and retain user anonymity and untraceability. Many existing protocols recommended for IoT contexts, on the other hand, do not match these requirements. A user authentication technique based on paring, this approach is vulnerable to attacks that target known session-specific temporary data, impersonation, privileged insider, and offline password guessing attacks, according to our findings. Furthermore, because their approach employs bilinear pairing, it necessitates a high level of computation and communication. A unique authentication system that overcomes these security issues in this paper. To be suitable in IoT contexts, the proposed approach solely employs hash and exclusive-or operations. The proposed protocol to current authentication protocols using informal and formal analytical approaches such as the BAN logic, real-or-random (ROR) model, and AVISPA simulation, and demonstrate the recommended protocol's improved performance and security. As a result, the suggested protocol is long-term and suited for real-world IoT scenarios.

Keywords: mutual authentication, MIM, lightweight, anonymity, IoT environment, BAN logic, ROR model, Avispa simulation, key agreement,

1. Introduction

IoT has emerged as a critical technology in business and industry, with applications in telecare systems, smart grids, intelligent transportation systems, and global- roaming systems [1–8] to improve people's lives. Medical equipment and sensors, for example, assess real-time monitoring of the patient's body temperature, blood pressure, and pulse transfer the information to a distant server in IoT-based applications systems (see Figure 1). Following that, users such as physicians and researchers utilise mobile devices (such as smart phones) to authenticate the server and access the information for diagnosis or study. Telecare technologies based on the Internet of Things can benefit patients while also advancing healthcare. In addition, the Internet of Things may be used in various settings to boost company productivity and industrial efficiency. Despite these benefits, however, a number of issues must be addressed. In IoT contexts, communication takes place across wireless channels, which are vulnerable to hacking. They can intercept messages and perform different attacks, such as replay, MIM attack, and impersonation assaults [9–11], as well as try to track down a user in order to gain sensitive information. Additionally, the effectiveness of the authentication mechanism should be evaluated to guarantee real-time mobile device connectivity with restricted computational power [12]. As a result, for long-term communication in IoT contexts, a safe and fast authentication mechanism is required. Recently suggested authentication systems in IoT contexts, on the other hand, have a number of security flaws and require a lot of work utilising the bilinear paring operations [14], scalar multiplication and

the elliptic curve cryptosystem (ECC) [13].These flaws may pose a threat to the network's long-term viability. In 2019, Raja ram [15] introduced a bilinear- pairing user authentication system. They said their system is secure from assaults and has a variety of security measures. However, we found that their system includes a number of security flaws that might be exploited in wireless networks. Because it employs bilinear pairing, their technique cannot ensure user anonymity and has a significant computational cost. As a result, we propose an enhanced authentication system that can address these concerns.

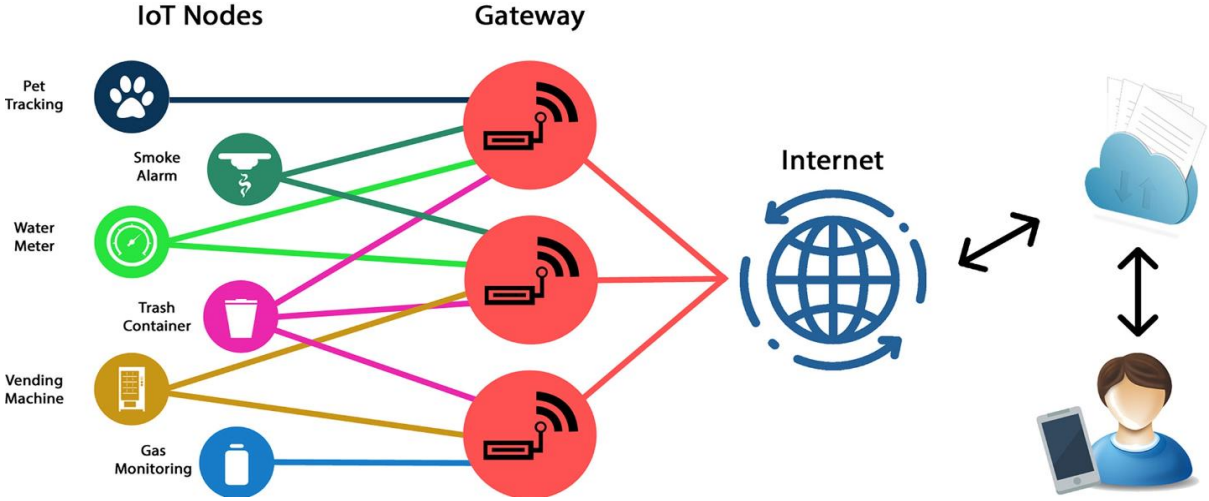

Figure 1: IoT Based Applications

1.1. Motivation

Each message in an IoT context is sent across public channels. Personal sensitive information may be contained in the messages, and if this information is exposed to an opponent, substantial privacy risks may arise. Furthermore, because IoT devices have limited processing capabilities, a high calculation cost might result in delays. As a result, for long-term IoT contexts, a safe and efficient authentication mechanism is required. We presented a user authentication mechanism based on pairings in 2019. There is no defence against offline guessing, impersonation, privileged insider, or known session-specific temporary information assaults. We mention the limits and drawbacks of previous investigations in addition. Several techniques employed elliptic curve multiplication and bilinear pairing, both of which are computationally intensive, rendering them unsuitable for IoT contexts. Furthermore, most schemes are vulnerable to attacks such as impersonation, off-line guessing, and privileged insider assaults, and are unable to provide authentication mechanisms include user anonymity and mutual authentication, or user un-traceability. Existing methods are not sustainable in IoT contexts as a result of these flaws, It led us to develop a new authentication system that fixes the issues with earlier work and offers security and effectiveness.

2. Related Works

Many authentication schemes for IoT contexts have been presented in recent years, developed a lightweight and anonymous authentication mechanism in 2018 [16]. They employed ECC for authentication and BAN logic to examine the scheme. They also used C++ to mimic computation and communication expenses. For IoT-based healthcare systems, [17] presented a three-factor user authentication mechanism. They were in charge of

establishing trust between medical experts and a cloud server. [18] Highlighted the existing methods' security and efficiency, and presented an ECC-based authentication technique for IoT contexts. To establish security and correctness, they used the AVISPA and ProVerif tools to formally examine the scheme. Many authentication schemes for IoT contexts have been presented in recent years. Authentication systems based solely on hash and exclusive-or operations have been proposed in several research. For dispersed systems, Kumari et al. [19] presented remote user authentication with two factors solution in 2014. They stated that their approach had a number of security features, including resistance to smart card theft and impersonation attacks system, however, is subject to smart card loss attacks, according to Kaul and Awasthi [20]. They suggested an improved authentication mechanism and used the AVISPA simulation tool to officially examine it. [21] shown that approach is not safe against offline guessing of passwords and de-synchronization attacks, and that it cannot ensure user anonymity. They presented a key agreement method based on biometrics. They do not, however, take into account session-specific transitory information attacks are well-known. [22] also claimed that Kaul and Awasthi's method is vulnerable to user impersonation attacks using a stolen smart card, and offered a lightweight authentication approach for IoT infrastructures. Their technique, on the other hand, does not account for known session-specific transitory information attacks and so cannot guarantee user anonymity.

As per the previous analysis a user authentication technique based on bi-linear pairing in 2019. They claimed that reciprocal authentication is possible and that their system is safe against offline guessing privileged insider attacks, and impersonation. Nevertheless, we discover that the plan is exposed to the aforementioned assaults, Lack of user anonymity, a known session-specific transitory information assault, and the aforementioned attacks. Because it employs bilinear pairing, their technique has a significant computational cost. We offer a safe, lightweight, and anonymous user authentication mechanism in this work that addresses the difficulties raised above and is suited for IoT contexts.

3. Proposed Scheme

User registration, login, authentication, and password are the initial steps, updating are all included in the proposed approach. The suggested scheme's notations are described in Table

Notation	Description
IDn, IDu, IDgw	IoT node,
IDu	User
IDgw	Gateway node
N1,N2,N3	Numbers
X,Y	Variables
Pkn,	Public Key Node
Pkgw,	Public Key Gateway
Pku	Public Key User
Inc	Increment Function

Table: 1 Notations

- IDn authenticates IDu on IDGW
- Chooses IDu,IDgw and generates nonce-1
- IDgw =>IDu with public key
- IDu->IDn will share data with a public key 1
- IDn=>IDgw send a nonce number

- IDgw=>IDn will check with nonce and public key 2
- IDn=>IDu receives a nonce number with Public key3

IDu starts communication with IDgw by generating a random number 1, later gateway (IDgw) with send a public key 1 with previous details to IDu from IDu to IDn data exchange is held with multiple nonce numbers (nonce-2,3,4), IDn to IDgw communication is held with a nonce number 5, later from IDgw to IDn verification is done with nonce 5 and public key 2,IDn to IDu

4. User Registration

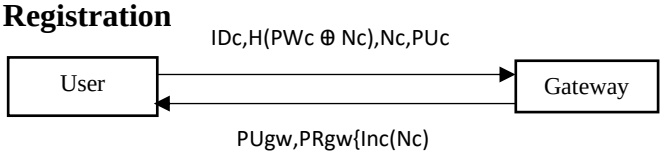

Fig 2: User registration Phase

In the User registration module user is registered via the gate way once the registration is completed then node also needs to be register in the next stage.

5. Node Registration

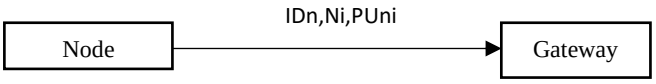

Fig 3: Node registration Phase

Once the registration of the node gets completed with gateway then authentication is going to happen via login in phase of login and authentication.

6. Phase of Login and Authentication

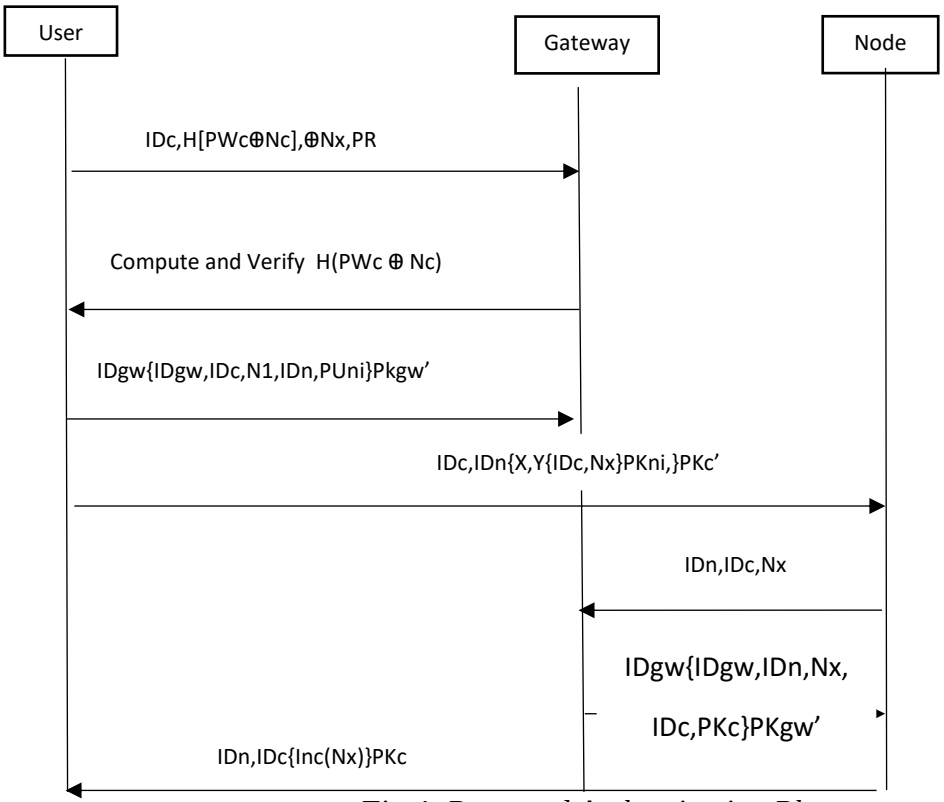

Fig 4: Proposed Authentication Phase

7. Formal Analysis Using Avispa Simulation

We use informal and formal analyses, such as the AVISPA, to assess the security of the proposed method protocol. By simulating the authentication protocol as code, AVISPA tool [23] may check to see if the authentication mechanism is secure from MITM and replay attacks. AVISPA is utilized as a formal verification tool in various authentication methods [24-26]. It is written in the "High-Level Protocol Specification Language" (HLPSL) and employs four back ends: "On-the-fly Model-Checker (OFMC)," "SAT-based Model-Checker (SATMC)," "Constraint Logic Based Attack Searcher (CL-AtSe),” shown in figure 6 and "Tree Automata Based on Automatic Approximations for the Analysis of Security Protocols (TA4SP)." The- HLPSL2IF converter transforms the intermediate format (IF) of HLPSL code into the output format (OF) shown in figure 5. The OF displays the simulation results, including "SUMMARY," "DETAILS," "PROTOCOL," "GOAL," "BACKEND," and "STATISTICS." The SUMMARY indicates if the method is fair, the BACKEND indicates the name of the back-ends, and STATISTICS indicates the assault trace's time.

```
role role_IDn(IDn:agent,IDu:agent,IDgw:agent,Pkn:public_key,Pkgw:public_key,Pku:public_key,Inc:hash_func,SND,RCV:channel(dy))
played_by IDn
def=
        local
                State:nat,Y:text,X:text,N3:text,N2:text
        init
                State := 0
        transition
                3. State=0 ∧ RCV(IDu.IDn.{X'.Y'.{IDu.N2'}_Pkn}_inv(Pku)) =|> State':=1 ∧ N3':=new() ∧ SND(IDn.IDu.N3')
                5. State=1 ∧ RCV(IDgw.{IDgw.IDn.N3.IDu.Pku}_inv(Pkgw)) =|> State':=2 ∧ SND(IDn.IDu.{Inc(N2)}_Pku)
end role

role role_IDu(IDn:agent,IDu:agent,IDgw:agent,Pkn:public_key,Pkgw:public_key,Pku:public_key,Inc:hash_func,SND,RCV:channel(dy))
played_by IDu
def=
        local
                State:nat,N1:text,Y:text,X:text,N2:text
        init
                State := 0
        transition
                1. State=0 ∧ RCV(start) =|> State':=1 ∧ N1':=new() ∧ SND(IDu.IDn.N1')
                2. State=1 ∧ RCV(IDgw.{IDgw.IDu.N1.IDn.Pkn}_inv(Pkgw)) =|> State':=2 ∧ N2':=new() ∧ Y':=new() ∧ X':=new() ∧ SND(IDu.IDn.{X'.Y'.{IDu.N2'}_Pkn}_inv(Pku))
                6. State=2 ∧ RCV(IDn.IDu.{Inc(N2)}_Pku) =|> State':=3
end role

role role_IDgw(IDn:agent,IDu:agent,IDgw:agent,Pkn:public_key,Pkgw:public_key,Pku:public_key,Inc:hash_func,SND,RCV:channel(dy))
played_by IDgw
def=
        local
                State:nat,N1:text,N3:text
        init
                State := 0

        transition
                1. State=0 ∧ RCV(IDu.IDn.N1') =|> State':=1 ∧ SND(IDgw.{IDgw.IDu.N1'.IDn.Pkn}_inv(Pkgw))
                4. State=1 ∧ RCV(IDn.IDu.N3') =|> State':=2 ∧ SND(IDgw.{IDgw.IDn.N3'.IDu.Pku}_inv(Pkgw))
end role

role session1(IDn:agent,IDu:agent,IDgw:agent,Pkn:public_key,Pkgw:public_key,Pku:public_key,Inc:hash_func)
def=
        local
                SND3,RCV3,SND2,RCV2,SND1,RCV1:channel(dy)
        composition
                role_IDgw(IDn,IDu,IDgw,Pkn,Pkgw,Pku,Inc,SND3,RCV3) ∧ role_IDu(IDn,IDu,IDgw,Pkn,Pkgw,Pku,Inc,SND2,RCV2) ∧ role_IDn(IDn,IDu,IDgw,Pkn,Pkgw,Pku,Inc,SND1,RCV1)
end role

role environment()
def=
        const
                hash_0:hash_func,pk3:public_key,pk1:public_key,u:agent,n:agent,gw:agent,pk2:public_key,inc:hash_func,auth_1:protocol_id
        intruder_knowledge = {}
        composition
                session1(n,u,gw,pk1,pk2,pk3,inc)
end role

goal
        authentication_on auth_1
end goal

environment()
```

Fig 5: user and session roles, context, and objective.

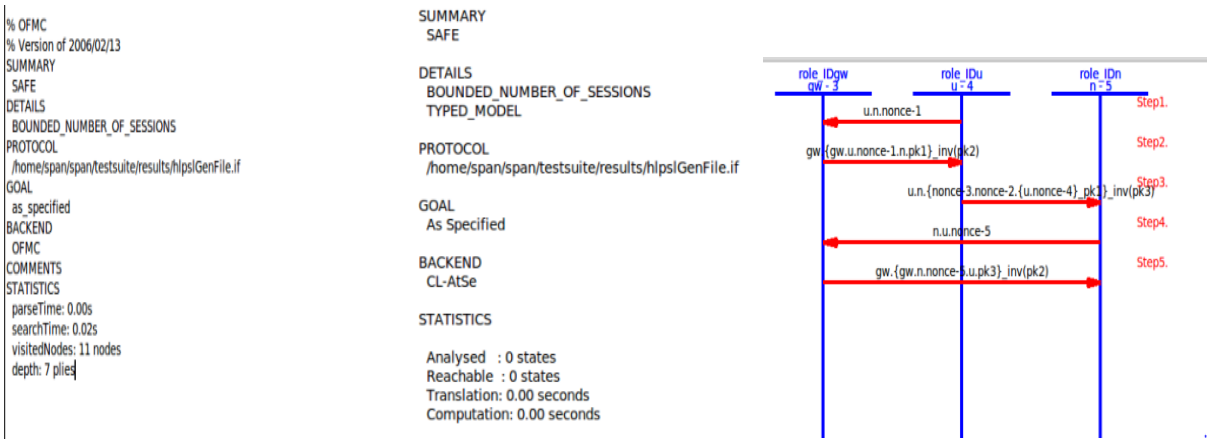

Fig 6: Results of the simulation using CL-AtSe and OFMC.

Conclusion

A safe, lightweight, and anonymous authentication system for IoT contexts in this work. The suggested protocol addressed the scheme's security weaknesses. During authentication, it exclusively employs hash and exclusive-or operations. As a result, it is much more effective than the system and other existing IoT authentication systems. Furthermore, the proposed protocol can prevent numerous attacks while also providing more security features than existing protocols. We used BAN logic analysis, RoR model to formally assess session key security, AVISPA simulation tool to show resilience to replay and man-in-the-middle (MITM) attacks, and BAN logic analysis to verify the proposed protocol. The suggested protocol is sustainable since it has a high level of security, requires little processing power, and might help reduce expenses by improving energy efficiency. As a result, the suggested protocol may be used in a variety of IoT scenarios. We want to put the proposed methodology into practise in future work.

References

1. Chen, C.M.; Xiang, B.; Liu, Y.; Wang, K.H. A secure authentication protocol for internet of vehicles. IEEE Access 2019, 7, 12047–12057. [CrossRef]

2. Bagga, P.; Das, A.K.; Wazid, M.; Rodrigues, J.J.P.C.; Kim, K.R.C.; Park, Y. On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system. IEEE Trans. Veh. Technol. 2021, 70, 1736–1751. [CrossRef]

3. Rathee, G.; Ahmad, F.; Sandhu, R.; Kerrache, C.A.; Azad, M.A. On the design and implementation of a secure blockchain-based hybrid framework for industrial Internet-of-Things. Inf. Process. Manag. 2021, 58, 102526. [CrossRef]

4. Nikooghadam, M.; Amintoosi, H.; Islam, S.H.; Moghadam, M.F. A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance. J. Syst. Archit. 2021, 115, 101955. [CrossRef]

5. Barka, E.; Dahmane, S.; Kerrache, C.A.; Khayat, M.; Sallabi, F. STHM: A secured and trusted healthcare monitoring architecture using SDN and blockchain. Electronics 2021, 10, 1787. [CrossRef] 6. Wazid, M.; Das, A.K.; Hussain, R.; Succi, G.; Rodrigues, J.J. Authentication in cloud-driven IoT based big data environment: Survey and outlook. J. Syst. Archit. 2019, 97, 185–196. [CrossRef]

7. Mahmood, K.; Akram, W.; Shafiq, A.; Altaf, I.; Lodhi, M.A.; Islam, S.H. An enhanced and provably secure multi-factor authentication scheme for Internet-of-Multimedia-Things environments. Comput. Elect. Eng. 2020, 88, 106888. [CrossRef] Sustainability 2021, 13, 9241 20 of 21

8. Belghazi, Z.; Benamar, N.; Addaim, A.; Kerrache, C.A. Secure WiFi-direct using key exchange for Iot device-to-device communications in a smart environment. Future Internet 2019, 11, 251. [CrossRef]

9. Banerjee, S.; Das, A.K.; Chattopadhyay, S.; Jamal, S.S.; Rodrigues, J.J.; Park, Y. Lightweight failover authentication mechanism for IoT-based fog computing environment. Electronics 2021, 10, 1417. [CrossRef]

10. Oh, J.; Yu, S.; Lee, J.; Son, S.; Kim, M.; Park, Y. A secure and lightweight authentication protocol for IoT-based smart homes. Sensors 2021, 21, 1488. [CrossRef]

11. Das, A. K.; Wazid, M.; Yannam, A.R.; Rodrigues, J.J.; Park, Y. Provably secure ECC-based device access control and key agreement protocol for IoT environment. IEEE Access 2019, 7, 55382–55397. [CrossRef]

12. Terminology for Constrained-Node Networks. Available online: https://datatracker.ietf.org/doc/draft-bormann-lwig-7228bis/ 06/ (accessed on 17 August 2020).

13. Miller, V.S. Use of elliptic curves in cryptography. In Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Linz, Austria, 9–11 April 1985; pp. 417–426.

14. Boneh, D.; Franklin, M. Identity-based encryption from the Weil pairing. In Advances in Cryptology; Springer: Berlin/Heidelberg, Germany, 2001; pp. 213–229.

15. Rajaram, S.; Maitra, T.; Vollala, S.; Ramasubramanian, N.; Amin, R. eUASBP: Enhanced user authentication scheme based on bilinear pairing. J. Ambient Intell. Humaniz. Comput. 2019, 11, 2827–2840. [CrossRef]

16. Chen, Y.; Martínez, J.F.; Castillejo, P.; López, L. A lightweight anonymous client–server authentication scheme for the internet of things scenario: LAuth. Sensors 2018, 18, 3695. [CrossRef] 17. Thakare, A.; Kim, Y.G. Secure and efficient authentication scheme in IoT environments. Appl. Sci. 2021, 11, 1260. [CrossRef]

18. Dhillon, P.K.; Kalra, S. Multi-factor user authentication scheme for IoT-based healthcare services. J. Reliab. Intell. Environ. 2018, 4, 141–160. [CrossRef]

19. Kumari, S.; Khan, M.K.; Li, X. An improved remote user authentication scheme with key agreement. Comput. Elect. Eng. 2014, 40, 1997–2012. [CrossRef]

20. Kaul, S.D.; Awasthi, A.K. Security enhancement of an improved remote user authentication scheme with key agreement. Wirel. Pers. Commun. 2016, 89, 621–637. [CrossRef]

21. Kang, D.; Jung, J.; Kim, H.; Lee, Y.; Won, D. Efficient and secure biometric-based user authenticated key agreement scheme with anonymity. Secur. Commun. Netw. 2018, 2018, 9046064 . [CrossRef]

22. Rana, M.; Shafiq, A.; Altaf, I.; Alazab, M.; Mahmood, K.; Chaudhry, S.A.; Zikria, Y.B. A secure and lightweight authentication scheme for next generation IoT infrastructure. Comput. Commun. 2021, 165, 85–96. [CrossRef]

23. AVISPA. Automated Validation of Internet Security Protocols and Applications. Available online: http://www.avispa-project.org/ (accessed on 17 August 2021).

24. Yu, S.; Lee, J.; Park, K.; Das, A.K.; Park, Y. IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment. IEEE Access 2020, 8, 167875–167886. [CrossRef]

25. Banerjee, S.; Odelu, V.; Das, A.K.; Chattopadhyay, S.; Park, Y. An efficient, anonymous and robust authentication scheme for smart home environments. Sensors 2020, 20, 1215. [CrossRef]

26. Kim, M.; Lee, J.; Park, K.; Park, Y.; Park, K.; Park, Y. Design of secure decentralized car-sharing system using blockchain. IEEE Access 2021, 9, 54796–54810. [CrossRef]