1. Alumuru Mahesh Reddy[1], 2.Dr.M.Kameswara Rao[2]

Koneru Lakshmaiah Education Foundation (1,2)

doi:10.15199/48.2024.01.35

A Lightweight Symmetric Cryptography based User Authentication Protocol for IoT based Applications

***Abstract**. The utilization of IoT is expanding across various domains, including tele-care, intelligent home systems, and transportation networks. In these environments, IoT devices generate data that is gathered on remote servers, requiring external users to authenticate themselves to access the data. However, existing authentication protocols for IoT fall short in meeting the crucial requirements of speed, security against multiple attacks, and ensuring user anonymity and un-traceability. Our research has identified that authentication techniques based on pairing are susceptible to attacks targeting temporary session-specific data, impersonation, privileged insiders, and offline password guessing. Moreover, these approaches relying on bilinear pairing demand extensive computation and communication resources. In order to address these security concerns, to propose a novel authentication system specifically designed for IoT scenarios. The proposed approach exclusively utilizes hash and exclusive-or operations to ensure suitability within IoT context are thoroughly evaluated the recommended protocol against existing authentication protocols, employing both informal and formal analytical routine like BAN logic, ROR model, and AVISPA simulation. Our findings demonstrate will suggest protocol not only enhances performance but also enhances security. To improved security measures, the suggested method stands as a reliable and durable solution for real-world IoT scenarios, addressing the inherent challenges posed by authentication requirements in IoT environments.*

***Streszczenie.** Wykorzystanie Internetu Rzeczy rozszerza się w różnych dziedzinach, w tym w teleopiece, systemach inteligentnego domu i sieciach transportowych. W takich środowiskach urządzenia IoT generują dane gromadzone na zdalnych serwerach, co wymaga od użytkowników zewnętrznych uwierzytelnienia się w celu uzyskania dostępu do danych. Jednakże istniejące protokoły uwierzytelniania dla IoT nie spełniają kluczowych wymagań dotyczących szybkości, bezpieczeństwa przed wielokrotnymi atakami oraz zapewnienia anonimowości użytkownika i braku identyfikowalności. Nasze badanie wykazało, że techniki uwierzytelniania oparte na parowaniu są podatne na ataki ukierunkowane na tymczasowe dane specyficzne dla sesji, podszywanie się, uprzywilejowane osoby poufne i odgadywanie haseł offline. Co więcej, podejścia te opierające się na parowaniu dwuliniowym wymagają rozległych zasobów obliczeniowych i komunikacyjnych. Aby rozwiązać te problemy związane z bezpieczeństwem, zaproponowano nowatorski system uwierzytelniania zaprojektowany specjalnie na potrzeby scenariuszy IoT. Proponowane podejście wykorzystuje wyłącznie operacje skrótu i wyłączności lub w celu zapewnienia przydatności w kontekście IoT. Zalecany protokół jest dokładnie oceniany pod kątem istniejących protokołów uwierzytelniania, wykorzystując zarówno nieformalne, jak i formalne procedury analityczne, takie jak logika BAN, model ROR i symulacja AVISPA. Nasze odkrycia sugerują, że protokół nie tylko zwiększa wydajność, ale także zwiększa bezpieczeństwo. Aby poprawić środki bezpieczeństwa, sugerowana metoda stanowi niezawodne i trwałe rozwiązanie dla rzeczywistych scenariuszy IoT, stawiając czoła nieodłącznym wyzwaniom stawianym przez wymagania uwierzytelniania w środowiskach IoT. (**Protokół uwierzytelniania użytkownika oparty na lekkiej kryptografii symetrycznej dla aplikacji opartych na IoT**)*

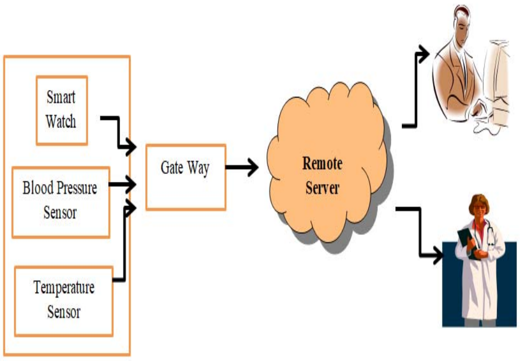
Keywords: MIM, anonymity, IoT node, BAN logic, ROR model, Avispa simulation, tele-care, remote server, IoT gateway.
Słowa kluczowe: MIM, anonimowość, węzeł IoT, logika BAN, model ROR, symulacja Avispa, teleopieka, zdalny serwer, bramka IoT

Introduction

The Internet of Things (IoT) has revolutionized various sectors, including healthcare, smart grids, transportation, and global roaming systems, enhancing people's lives [1-8]. In IoT-based telecare systems, for instance, medical equipment and sensors continuously monitor patients' vital signs and transmit the data to a remote server (as depicted in Figure 1). Subsequently, authorized users such as physicians and researchers employ mobile devices like smartphones to authenticate the server and have access to the data for identifying or for research. Leveraging IoT in tele-care systems holds great potential for improving healthcare outcomes. Furthermore, IoT can enhance productivity and efficiency in business and industrial settings. However, several challenges need to be addressed.

Wireless communication channels, commonly used in IoT environments, are susceptible to various security threats, including message interception, replay attacks, Man-in-the-Middle attacks, and impersonation attacks [9-11]. Additionally, there is a concern regarding user privacy and the potential leakage of sensitive information. Furthermore, the authentication mechanism must be efficient enough to accommodate resource-constrained devices like mobile devices with limited computational power [12]. As a result, a reliable and efficient authentication technique is required for ensuring long-term communication in IoT scenarios.

Existing authentication systems proposed for IoT environments suffer from security vulnerabilities and impose high computational overhead due to the use of bilinear pairing operations [14], scalar multiplication, and the elliptic curve cryptosystem (ECC) [13]. These weaknesses pose risks to the long-term viability of the network. In 2019, Raja Ram introduced a bilinear-pairing-based user authentication system, claiming its security and robustness. However, our analysis reveals several security flaws in their system that could be exploited in wireless networks. Moreover, the use of bilinear pairing in their approach fails to guarantee user anonymity and imposes significant computational costs.



Fige 1: IoT Based Tele-care Circumstances

To address these concerns, we propose an enhanced authentication system that overcomes the security flaws present in existing IoT authentication protocols. Our solution ensures both security and efficiency by utilizing alternative cryptographic techniques. We focus on maintaining user anonymity while minimizing the computational burden. By doing so, our proposed authentication system addresses the fore mentioned challenges, providing a secure and fast mechanism for long-term communication in IoT environments.

Literature Survey

In an IoT context, messages are broadcast through open channels, These conversations may also include valuable sensitive data. If this information is exposed to malicious adversaries, it can lead to significant privacy risks. Additionally, considering the limited processing capabilities of IoT devices, high computational costs can cause delays. Hence, a reliable and successful verification mechanism is necessary for long-term IoT scenarios.

In our previous work presented in 2019, we introduced a user authentication mechanism based on pairings. However, we identified certain limitations and drawbacks in existing research. Specifically, the previous investigations failed to provide defense against offline guessing attacks, impersonation attacks, privileged insider attacks, and known session-specific temporary information attacks. Additionally, many of the techniques employed elliptic curve multiplication and bilinear pairing, both of which are computationally demanding and unsuitable for IoT contexts. Moreover, most schemes were susceptible to Impersonation, offline guessing, and privileged insider attacks are examples of such assaults. They also lacked key features like user anonymity, mutual authentication, and user un traceability. Considering these flaws, the existing methods were not sustainable for IoT environments.

Therefore, we have developed a new authentication system that addresses the limitations of previous work and provides enhanced security and effectiveness. Our system overcomes the identified issues and ensures robust protection. By incorporating novel approaches, we have achieved improved security against various attacks while maintaining efficiency. Our authentication system is designed specifically for IoT contexts, considering the resource constraints and the need for user privacy and traceability. Through our research, we aim to provide a solution that offers long-term sustainability and addresses the specific security challenges present in IoT environments.

Related Works

In recent years, there have been numerous authentication schemes proposed for IoT contexts. For instance, in 2018, a lightweight and anonymous authentication mechanism was developed [16]. The scheme utilized Elliptic Curve Cryptography (ECC) for authentication and employed BAN logic to assess its security. Computation and communication costs were simulated using the C++ programming language. This particular scheme aimed to provide a lightweight and anonymous authentication solution for IoT applications.

In the domain of IoT-based healthcare systems, a three-factor user authentication mechanism was introduced [17]. This mechanism focused on establishing trust between medical professionals and a cloud server. Its purpose was to ensure secure and reliable authentication in healthcare scenarios, leveraging IoT technologies.

Another study [18] emphasized the importance of security and efficiency in authentication schemes for IoT contexts. They presented an authentication method based on ECC technique specifically tailored for IoT domain. To validate the scheme's security and correctness, the researchers employed formal analysis tools such as AVISPA and ProVerif.

Overall, the past few years have witnessed the introduction of several authentication schemes dedicated to IoT contexts. These schemes address the unique challenges posed by IoT environments and strive to provide secure, lightweight, and efficient authentication mechanisms for various IoT applications.

In several research studies, authentication systems based solely on hash and exclusive-or operations have been proposed. For instance, [19] introduced in 2014, a two-step remote user authentication solution for dispersed systems was released. They stated a method was secure, includes resilience to electronic card theft and fraud attempts. However, the system was subject to smart card loss attacks. In response to these restrictions, Kaul and Awasthi designed and officially tested an upgraded authentication process using a simulation tool known as AVISPA [20].

Furthermore, [21] demonstrated that Kaul and Awasthi's approach was not secure in the face of off-line password guessing assaults and desynchronization attacks. Additionally, it could not guarantee user anonymity. To address these shortcomings, they presented a key agreement method based on biometrics. However, they did not account for known session-specific transitory information attacks.

Another study by [22] criticized the vulnerability of Kaul and Awasthi's method to Threats on user impersonation with a stolen smart card. They proposed a lightweight authentication approach specifically designed for IoT infrastructures. However, similar to previous works, their technique did not take into account existing session-specific transitory insights attacks, consequently, could not ensure user anonymity.

It is evident that the authentication mechanisms discussed in these studies have made attempts to improve security and address specific challenges. However, each approach has its limitations, such as vulnerability to certain attacks or the inability to provide user anonymity. Future research efforts should consider these shortcomings and aim to develop comprehensive authentication systems that effectively address known vulnerabilities while ensuring user privacy and security.

In a previous analysis, a user authentication technique based on bilinear pairing was proposed in 2019. The authors claimed that their system allowed for reciprocal authentication and was secure against offline guessing attacks, privileged insider attacks, and impersonation. However, upon further investigation, it was discovered that their scheme was vulnerable to the mentioned attacks, lacked user anonymity, and did not address the issue of known session-specific transitory information attacks. Additionally, the use of bilinear pairing in their approach resulted in significant computational costs.

To overcome these challenges and provide an improved authentication mechanism suitable for IoT contexts, we present a secure, lightweight, and anonymous user authentication solution in our work. Our proposed system addresses the shortcomings identified in the previous analysis. It offers enhanced security against various attacks, ensures user anonymity, and mitigates the risks associated with known session-specific transitory information attacks. Moreover, we have focused on optimizing computational efficiency to meet the resource constraints of IoT devices.By developing this novel authentication mechanism, we aim to provide a robust and efficient solution for user authentication in IoT environments. Our approach tackles the identified challenges and provides the necessary security and privacy features required for IoT contexts.

Proposed Approach

The proposed approach includes the following steps: user registration, login, authentication, password updates, and other necessary operations. The notations used in the scheme are defined in Table 2 to provide clarity and understanding of the proposed mechanism.

Table: 1 Notations

Notation	Description
Idn	IoT node
Idu	User
Igw	Gateway node
n1,n2,n3	Numbers
x,y	Variables
Pukn,	Public Key Node
Pukgw	Public Key Gateway
Puku	Public Key User
In	Increment Function

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

User Registration

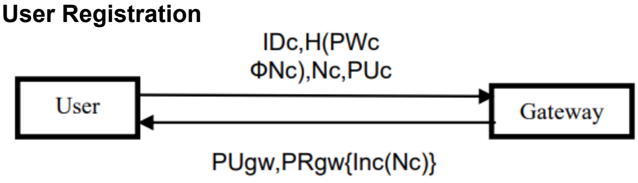


Fig 2: User registration Phase

In the User registration module, the user is first registered through the gateway. This involves providing necessary information, such as username, password, and any other required details. The registration process validates the user's information and creates a unique user profile within the system. Once the user registration is successfully completed, the next stage involves registering the node. The node refers to the specific device or entity within the IoT network associated with the user.

This registration step is essential for establishing the connection and association between the user and the corresponding IoT device or node. During node registration, relevant information about the device, such as its identifier or serial number, may be recorded and linked to the user's profile.

This allows the system to recognize and authenticate the device when it communicates or interacts within the IoT network.

Node Registration

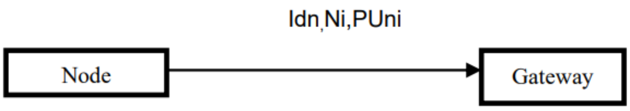


Fig 3: Node registration Phase

Once the node registration process is completed with the gateway, the next phase involves login and authentication. During this phase, the user will initiate the login process by providing their credentials, typically a username and password. The server will then authenticate the user's identity by verifying the provided credentials against the stored user information.

The authentication process may involve various security measures, such as encryption, hashing, and secure communication protocols, to ensure the confidentiality and integrity of the login credentials. The server will compare the provided credentials with the registered user information and determine whether the login attempt is valid.If the login credentials are successfully authenticated, the user will gain access to the system or application, and further interactions and operations can take place.

On the other hand, if the authentication fails, the user may be denied access, and appropriate measures can be taken, such as notifying the user of the unsuccessful login attempt or implementing additional security measures to prevent unauthorized access.

Overall, the login and authentication phase is a crucial step in ensuring the security and integrity of the IoT system, as it verifies the user's identity and grants appropriate access privileges based on the authentication outcome.

Phase of Login and Authentication

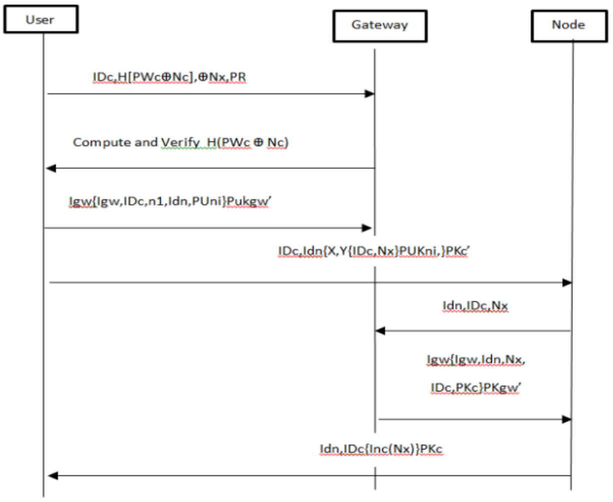


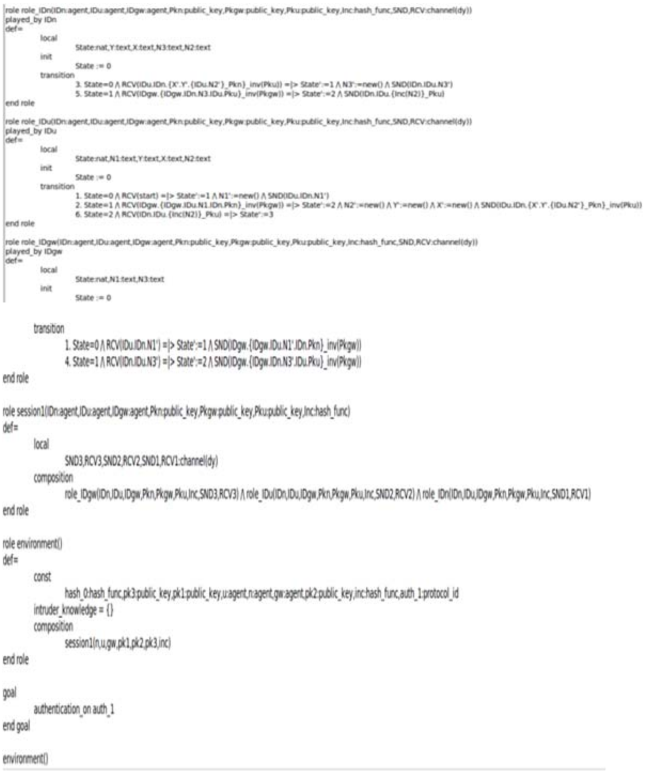
Fig 4: Proposed Authentication Phase

Formal Analysis Using Avispa Simulation

To assess the security of the proposed authentication protocol, both informal and formal analyses are employed, including the use of the AVISPA tool [23]. AVISPA is a formal verification tool commonly used to verify the security of authentication methods [24-26]. It operates by simulating the authentication protocol as code and checking for security vulnerabilities, such as MITM (Man-in-the-Middle) and replay attacks.

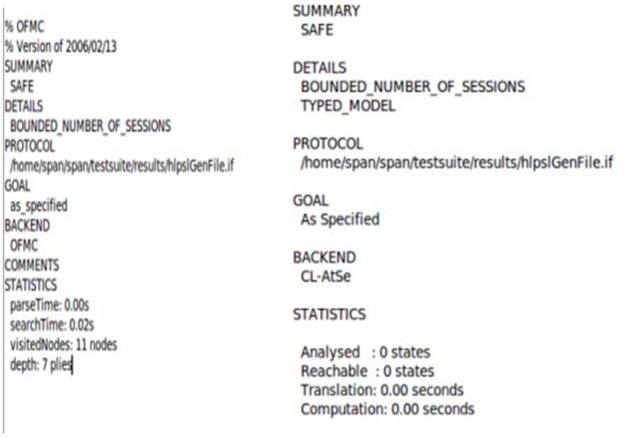
AVISPA carry out the "High-Level Protocol Specification Language" (HLPSL) offers four back ends for analysis: "On-the-fly Model-Checker (OFMC)," "SAT-based Model-Checker (SATMC)," "Constraint Logic Based Attack Searcher (CL-AtSe)," along with "Tree Automata Based on Automatic Approximations for the Analysis of Security Protocols (TA4SP)." HLPSL2IF converter is utilized to transform the HLPSL code into an output format (OF), which provides simulation results. The output format (OF) generated by AVISPA includes several sections, such as "SUMMARY," "DETAILS," "PROTOCOL," "GOAL," "BACKEND," and "STATISTICS." The SUMMARY section indicates whether the method is considered secure or not. The BACKEND section displays the name of the back ends used in the analysis, and the STATISTICS section provides information about the time taken to trace potential attack scenarios.

By employing AVISPA and its analysis capabilities, the proposed authentication protocol can be rigorously evaluated for its security against different types of attacks. The tool provides valuable insights into the protocol's strengths and weaknesses, helping to refine and enhance its security properties.



```
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.



```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/hlpslGenFile.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.02s
 visitedNodes: 11 nodes
 depth: 7 plies
```

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/hlpslGenFile.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 0 states
  Reachable  : 0 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds
```

Conclusion

In this work, a solution for safe, small in size, and anonymous authentication for IoT contexts has been put forward. The suggested protocol addresses the security weaknesses identified in existing schemes. The protocol exclusively has the verification procedure, hash and exclusive-or operations are used, making it is additionally effective compared to other IoT authentication systems. Moreover, the proposed protocol provides enhanced security features and can prevent various attacks. To evaluate its security, the protocol underwent analysis using BAN logic, RoR model for session key security, and AVISPA simulation tool to demonstrate resilience against replay and man-in-the-middle (MITM) attacks. The put up forward validity was also verified through BAN logic analysis.

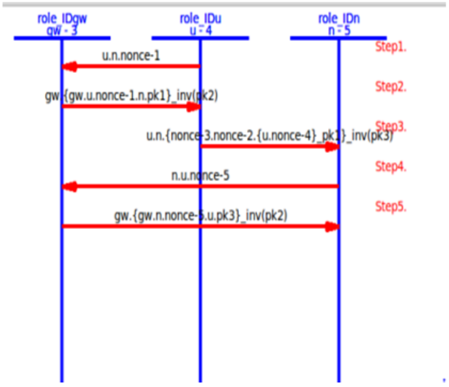

role_IDgw
gw - 3
role_IDu
u - 4
role_IDn
n - 5
Step1.
u.n.nonce-1
Step2.
gw.{gw.u.nonce-1.n.pk1}_inv(pk2)
Step3.
u.n.{nonce-3.nonce-2.{u.nonce-4}_pk1}_inv(pk3)
Step4.
n.u.nonce-5
Step5.
gw.{gw.n.nonce-5.u.pk3}_inv(pk2)

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

The suggested protocol is designed to be sustainable, as it offers a high level of security while requiring minimal processing power. This can potentially contribute to reduced expenses and improved energy efficiency in IoT environments. Therefore, the protocol is applicable in a wide range of IoT scenarios.In future work; the proposed methodology will be implemented to validate its effectiveness in real-world applications. The aim is to deploy the protocol and further assess its performance and security in practical IoT settings.

***Authors**: 1.Research Scholar Mr.Alumuru Mahesh Reddy, Department of ECM,KLEF(Koneru Lakshmaiah Education Foundation). Green Fields, Vaddeswaram, Andhra Pradesh 522302,E-mail: alumuru.mahesh@gmail.com.*

2. Associate Professor, Dr M.Kameswarao Department of ECM,KLEF(Koneru Lakshmaiah Education Foundation). Green Fields, Vaddeswaram, Andhra Pradesh 522302,E-mail: kamesh.manchiraju@kluniversity.in

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]