Security Analysis and Improvements of Communication Protocol in the Internet of Things

[1]**Vinod Kumar Singh**, Research Scholar, Rama University Uttar Pradesh, Kanpur
[2]**Hari Om Sharan**, Professor, Rama University Uttar Pradesh, Kanpur
[2]**C.S. Raghuvanshi**, Professor, Rama University Uttar Pradesh, Kanpur
drsharan.hariom@gmail.com

Abstract:

Internet of Things has recently emerged as the cutting-edge technology that is heavily influencing commercial, healthcare, and military applications. Since anything connected to the internet is susceptible to cyber attacks and a target for hackers, wireless communications are particularly sensitive to security risks. Multiple Internet of Things problems are posing security risks and preventing End-to-End encryption during data transmission. The majority of Internet of Things devices now in use don't have improved setups or security procedures, which makes them vulnerable to hacker attacks. For all Internet of Things devices, advanced security standards cannot be used. For the Internet of Things platform, this study proposed a safe authentication system that keeps track of security risks and ensures the security of Internet of Things devices. An assessment of the suggested procedure is provided, demonstrating its capacity to address a range of security concerns.

Keywords: Internet of Things, Communication Protocol, Cyber attacks, Encryption, Access Control

DOINumber: 10.14704/NQ.2022.20.12.NQ77075 **NeuroQuantology2022;20(12): 937-946**

Introduction:

A network that connects common objects is known as the Internet of Things (IoT) or the Internet of Objects. With the incorporation of things into daily life through embedded technologies, the IoT expands the current Internet into a larger network. Intelligent items will interact with one another in a network. IoT applications are currently present in many areas of daily life, such as the healthcare industry, transportation, utilities, smart homes, and smart appliances. The evolution of wireless communication devices and technology has given rise to the Internet of Things, which is widely available and used in our society today. Our culture is embracing the IoT in many different ways, and as a result, daily convenience is rising as a result of individuals being able to control and utilize devices anywhere and at any time. However, there have also been instances of this advancement being exploited. A number of security incidents, including hacking, the release of private information, and the use of DDoS assault to target the IoT device or network itself. IoT devices really require substantially less processing power and memory than modern PCs, smart phones, and tablets, which makes it difficult to deploy the same security methods on them (1,2). In fact, a large-scale DDoS attack utilizing an IoT device occurred on Dyn, which hosts Internet domains, and this attack forced numerous popular websites, including Twitter, Netflix, and Amazon, to be offline for a considerable amount of time. There was a time when I was unable to. In the event of a DDoS attack, it was a frequently employed attack technique, but it was primarily a PC-based attack technique. However, this instance proved that assaults using smart devices, like IP cameras, CCTV (Closed Circuit Television), and home IoT devices for daily household appliances, are feasible. A typical HTTP fault attack that intended to overwhelm cloud services with resources was also discovered through an embedded device connected to Internet Explorer. In one case, IP cameras from all around the world that were running the busybox toolkit and Linux embedded were used to launch an attack that could send up to 20,000 queries per second. It supposedly fell short. When it comes to computers, harmful codes are typically infected through software self-vulnerabilities or social engineering techniques, however in the case of the attack method mentioned above; it is simple to counteract the attack because the Internet can be accessed via Telnet or SSH. Additionally, there are issues with management. As the current initial authentication value, the ID and password combination "ID: root. It is challenging to mount enough memory or power since the device size is constrained by the intended purpose. Due to the simplicity of physical access, installing a security solution and safeguarding authentication and encryption keys becomes challenging. As a result, it is anticipated that DDoS assaults or the disclosure of private information would continue to happen in the future. By 2022, it is anticipated that 35 billion gadgets will be online, as the Internet of Things (IoT) is expected to continue to grow. Continuous confusion may happen if vulnerability management is not carried out [3–8]. As a result, we suggest an authentication and key exchange scheme in this paper for secure communication in an IoT environment, as well as an authentication scheme that can be used by devices on which the current security protocols are difficult to implement due to memory and processing power constraints.

The Internet of Things (IoT) is an emerging global information service platform that uses sensor nodes and smart devices to enable a wide range of envisioned and implemented use cases [9]. According to the ITU concept, the core IoT design may be understood as essentially any physical object worldwide would be able to precisely, "things" are not changed into computers, but they have tiny computer's skills in a little footprint and wiser nature [10]. The Internet of Things (IoT) uses a variety of technologies, including those related to architecture, sensor/identification, coding, transmission, data processing, networks, discovery, etc. In 1999, when discussing supply chain management, Kevin Ashton, cofounder and executive director of the Auto-ID Center at MIT, was the first to use the term "Internet of Things" [11]. However, new IoT network applications, such e-healthcare and transportation utilities, have expanded this notion over the past ten years [12]. The development of the Internet of Things (IoT) began with the fusion of wireless technologies, developments in micro electromechanical systems (MEMS), and digital electronics, which led to the creation of tiny devices with wireless communication, sensing, and computation capabilities. The connection or relationship between humans and machines is increasingly taken into account in the Internet of Things age as machines become smarter and begin to take on more human jobs. In this scenario, humans must trust the machine and feel secure. Accordingly, a thing could be a patient with a medical device to provide real-time monitoring in a healthcare application or a cow with an accelerometer for movement in a farm setting. Security and privacy issues are the most difficult subjects in such a networked system of miniature "things" [14–18]. The main components to solve security and privacy issues in computer networks [28-41] are authentication and access control systems [19–27]. They can stop unauthorized users from accessing resources, stop authorized users from accessing resources in an unauthorized way, and allow approved users to access resources. It is crucial to consider efficiency, security scalability, and market-oriented computing, power resource, and storage aspects while developing an IoT infrastructure in order to give the best possible services to customers or users. Jing et al. suggested an IoT-based technique for authentication and access management in 2012 [28]. They build a workable protocol for the Internet of Things in addition to analyzing the various authentication and access control techniques now in use. Their plan states that the authentication protocol's emphasis was on quick and effective secure key establishment based on ECC. They used the Role Based Access Control (RBAC)-based authorization mechanism for the access control policy, taking into account the specific roles and applications that the things in the connected IoT network play. In this research, we demonstrate how their proposed security evaluation is impractical in a real-world setting and how their scheme is expensive for the IoT sensor nodes' overall communication process.

Review of Literature:

IoT is getting more and more attention quickly because it can collect and send information by connecting everything to the internet. To provide the best service possible in the area, a specific number of research projects are being conducted at various universities and labs. One of the research areas being looked into is security, and additional solutions have been put out. We review the works that have been done in this field in this part. In the context of the Internet of Things, where mobile nodes must be verified by the cluster in order to conduct communication, Jingjun and Liangmin [42] presented a rapid identity authentication protocol for mobile nodes. This kind of protocol is practical and offers privacy protection. The suggested protocol, which quickly implements identification authentication and privacy protection, is based on the Veronoi [43] network model and incorporates a valid request message and a response authentication message. The authors also examined the security of the protocol before formalizing it in applied pi calculus, a language for describing concurrent processes and their interactions. It expands the pi calculus by giving users the option to represent cryptographic primitives using equation theory and signatures. This serves to demonstrate how well the protocol protects privacy. The authors discovered that their protocol has reduced communication overhead, is sufficiently safe, and offers additional privacy protection elements compared to related single-step protocols like the basic hash protocol and OSK protocol. For multimedia applications with key features including traffic analysis, security requirements, and traffic scheduling, Liang et al [44]'s developed security-critical multimedia service architecture. One of the first security-conscious traffic management solutions for such IoT applications, according to the authors, is their suggestion. The following are the important elements of the suggested protocol: key management [45–47], batch rekeying, authentication, and watermarking. The proposed methodology for the authentication process uses a variety of techniques, from mutual authentication between the server and user based on access control, ability certificates, and mutual authentication to the use of access control and capability certificates [48, 49]. In general, watermarking serves to identify the source of the content, track down unlawfully distributed items, and bar unauthorized access to the content [50]. Three modes of operation are recommended [51] to meet the needs of various multimedia applications: periodic batch rekeying, periodic batch leave rekeying, and periodic batch join rekeying. A communication protocol for RFID systems in the Internet of Things was proposed by Gao et al. [52] and its security was demonstrated using the random oracle approach [53]. Readers, tags, and RFID middleware make up the bulk of the suggested security model for Internet of Things (IoT) RFID systems. The EPC of each object in the system is distinct. The random oracle model is used to define the RFID system model in the Internet of Things [54]. The article suggests the SPAP protocol, which makes use of XOR, one-way hashing, and symmetric encryption. As demonstrated by the random oracle model, SPAP can accomplish internal security, ownership transfer of tags, and mutual authentications. In addition, SPAP can resist retransmission and some common assaults. The SPAP protocol performs well, according to the findings of the safe performance analysis. For the perception layer of the Internet of Things, Ye et al. [55] have more recently proposed an effective authentication and access control scheme that focuses on quick and easy mutual authentication and secure key establishment based on ECC, which has significantly lower storage and communication overheads. The access control policy has implemented the ABC-based authorization approach. The user is described as a visitor in the perception layer and includes devices like as mobile phones and smart computers. Their architecture design is primarily based on the concept of a base station (BS) which collects the data and manages the sensor nodes. Finally, the organization in responsibility of producing and managing the attribute information is known as the attribute authority (AA). To enable mutual authentication between users and nodes and fine-grained access control, an effective ECC-based authentication method and attribute-based access control policy were put forth. Mutual authentication, whose procedure is simple to address the resource-constrained issue of the IoT perception layer, assures the security of communication between user and nodes. Flexible fine-grained access control can be achieved by using user attribute certificates in the access control authority to access the data.

Suggestions for Changes:

The proposed changes have two parts: the registration stage and the validation stage. There is also a third, very important part called "password recovery or change." After analyzing the IoT scheme proposed by Jing et al., this section shows the suggested improvements. To make up for this security hole, we've come up with security patches that fix the flaws in Jing et alplan. .'s Before going into detail about the proposed changes, some assumptions are made that should not be broken when the plan is put into action.

Performance and Security Analysis:

It was demonstrated in [56–59] that security services are taken into account more when analyzing the data and network security, so in this analysis we assume that an adversary may intercept M1, M2, and M3 at any time. In this section, we present our proposed protocol evaluation in terms of security analysis. Additionally, we make the assumption that an adversary can steal a user device or hack passwords, but not both at once. According to the available literature, it can be challenging to extract secrets from a smart card's memory, hence several firms that make smart cards offer defenses against the possibility of such side channel assaults. Based on the aforementioned hypotheses, an attacker might carry out specific assaults to thwart the suggested protocol. Security Assessment It is utilized in this area to assess network security. Analyze how safe it is to launch attacks against well-known security holes. By contrasting the perfection with previous investigations, the quality was confirmed.

Mutual Authentication

In this article, we continue the ID/PW subscription process by joining the authentication centre utilizing encryption mechanism. Random number values are traded during this procedure, and these values are eventually utilized to update authentication and key values. Additionally, the polynomial f(k) is transmitted to the user and the IoT device, respectively, in the case of the authentication centre, for the subsequent authentication process. After initial authentication, mutual authentication is possible by having a verification procedure with this polynomial value. The polynomial f(k) is utilized in the subsequent authentication process to directly authenticate the user and the IoT device, respectively, as the authentication centre manages the authentication process and enables secure authentication.

Reuse Attack

By illegal users, device-device and person this is an exploit that takes a message produced during the communication process between two devices and reuses it. Through the constant exchange of random numbers, it is possible to validate the previous transmission value even if the message has been stolen. Additionally, since the timestamp is assumed to be transmitted during the authentication procedure in this study, it is feasible to confirm the accuracy of the data sent earlier.

Message Forgery Attack:

This is an attack in which an unauthorized user intercepts a message created during the communication process between a device and a person's device, forges or modifies the message, and transmits it for the attacker's intended use. During data transfer, encryption It generates and transmits the cypher text using the key, therefore unless an attacker gets the key, it is secure against message forging attempts.

Sniffing:

Messages created throughout the communication process are encrypted using a secret key as one of the attack techniques to peek at messages carried on the network. Even if an attempt is made to peep into messages by sniffing by continuously changing the key, encryption will prevent this. Since it can only see the message, it is protected against the attack.

Spoofing:

It is an attack strategy that presents network users' and devices' identity data as that of an authorized user in an effort to trick the adversary. Pre-communication involves performing the authentication method, and even if a spoofing attack takes place, the secret that each node shared during the first authentication operation will prevent it. Given that the amount is unknown, it is secure from assault.

Conclusion:

The development of hardware and internet technology offers people many advantages, but regrettably, a lot of security threat scenarios are happening at the same time. The performance of IoT devices has suffered greatly as a result of the expansion of malware and hacking techniques employed in the current PC environment to IoT devices. Applying the security protocol on communication protocol of the current PC environment is challenging due to memory and power constraints. So, as can be seen from the article, a security protocol was built while taking into account the IoT call's features and the suitability for both security and performance was verified by performance evaluation. Therefore, it is anticipated that it will be able to provide an effective security system in the future Internet environment if the proposed protocol is implemented.

References:

1. Kolias, Constantinos, et al. DDoS in the IoT: Mirai and other botnets. Computer, 2017, 50.7: 80-84. DOI: https://doi.org/10.1109/mc.2017.201
2. Yang, Yuchen, et al. A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal, 2017, 4.5: 1250-1258. DOI: https://doi.org/10.1109/jiot.2017.2694844
3. Frustaci, Mario, et al. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of Things Journal, 2017, 5.4: 2483-2495. DOI: https://doi.org/10.1109/jiot.2017.2767291
4. Khan, Minhaj Ahmad; SALAH, Khaled. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 2018, 82:395-411. DOI: https://doi.org/10.1016/j.future.2017.11.022
5. Bkamble, Ashvini; BHUTAD, Sonali. Survey on Internet of Things (IoT) security issues & solutions. In: 2018 2nd International Conference on Inventive Systems and Control (ICISC). IEEE, 2018. pp. 307-312. DOI: https://doi.org/10.1109/icisc.2018.8399084
6. Samie, Farzad; BAUER, Lars; HENKEL, Jörg. IoT technologies for embedded computing: A survey. In: Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis. ACM, 2016. p. 8.DOI: https://doi.org/10.1145/2968456.2974004
7. Saha, Himadri Nath; MANDAL, Abhilasha; SINHA, Abhirup. Recent trends in the Internet of Things. In: 2017 IEEE 7th annual computing and communication workshop and conference (CCWC). IEEE, 2017. pp. 1-4.
8. Sohoel, Halldis; JAATUN, Martin Gilje; BOYD, Colin. OWASP Top 10-Do Startups Care. In: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, 2018. pp. 1-8. DOI: https://doi.org/10.1109/cybersecpods.2018.8560666
9. Atzori, L.; Iera, A.; Morabito, G. The Internet of things: A survey. Comput. Netw. 2010, 54, 2787–2805.
10. ITU. The Internet of Things; ITU Report: Genf, Switzerland, 2005.
11. Ashton, K. That ‗Internet of Things" thing. Available online: http://www.rfidjournal.com/ (accessed on 22 June 2009).
12. Sundmaeker, H.; Guillemin, P.; Friess, P.; Woelfflé, S. Vision and Challenges for Realising the Internet of Things; European Commission—Information Society and Media: Brussels, Belgium, 2010.

13. Gartner‘s Hype Cycle Special Report for 2011, Gartner Inc., 2012. Available online: http://www.gartner.com/technology/research/hype-cycles/ (accessed on 10 August 2011).
14. Weber, R.H. Internet of things–new security and privacy challenges. Comput. Law Secur. Rev. 2010, 26, 23–30.
15. Huang, H.; Wang, H. Studying on Internet of things based on fingerprint identification. In Proceedings of 2010 International Conference on Computer Application and System Modeling, Taiyuan, China, 22–24 October 2010; pp. 628–630.
16. Xiong, L.; Zhou, X.; Liu, W. Research on the architecture of trusted security system based on the Internet of things. In Proceedings of the 4th International Conference on Intelligent Computation Technology and Automation, Shenzhen, China, 28–29 March 2011; pp. 1172–1175.
17. Wang, K.; Bao, J.; Wu, M.; Lu, W. Research on security management for Internet of things. In Proceedings of 2010 International Conference on Computer Application and System Modeling, Taiyuan, China, 22–24 October 2010; pp. 133–137.
18. Sarma, A.; Girao, J. Identities in the future Internet of things. Wirel. Pers. Commun. 2009, 49, 353–363.
19. Du, X.; Guizani, M.; Xiao, Y.; Chen, H. A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks. IEEE Trans. Wirel. Commun. 2009, 8, 1223–1229.
20. Vapen, A.; Byers, D.; Shahmehri, N. 2-clickAuth–optical challenge-response authentication. In Proceedings of 2010 International Conference on Availability, Reliability and Security, Krakow, Poland, 15–18 February 2010; pp. 79–86.
21. Benenson, Z.; Gartner, F.; Kesdogan, D. An algorithmic framework for robust access control in wireless sensor networks. In Proceedings of the Second European Workshop on Wireless Sensor Networks, Istanbul, Turkey, 31 January–2 February 2005; pp. 158–165.
22. Le, X.H.; Lee, S.; Butun, I.; Khalid, M.; Sankar, R. An energy efficient access control for sensor networks based on elliptic curve cryptography. J. Commun. Netw. 2009, 11, 599–606
23. Shen, Y.; Ma, J.; Pei, Q. An access control scheme in wireless sensor networks. In Proceedings of the IFIP International Conference on Network and Parallel Computing Workshops, Liaoning, China, 18–21 September 2007; pp. 362–367.
24. Wong, K.; Zheng, Y.; Cao, J.; Wang, S. A dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, Taichung, Taiwan, 5–7 June 2006.
25. Tseng, H.; Jan, R.; Yang, W. An improved dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE Global Communications Conference, Washington DC, USA, 26–30 November 2007; pp. 986–990.

26. Gravina, R.; Guerrieri, A.; Fortino, G.; Bellifemine, F.; Giannantonio, R.; Sgroi, M. Development of Body Sensor Network Application Using SPINE. In Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Singapore, 12–15 October 2008.
27. Sulaiman, R.; Sharma, D.; Ma, W.; Tran, D. A Security Architecture for e-Health Services. In Proceedings of the 10th International Conference on Advanced Communication Technology, Gangwon-Do, Korea, 17–20 February 2008.
28. Jing, L.; Xiao, Y.; Chen, C.L.P. Authentication and Access Control in the Internet of Things. In Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops, Macau, China, 18–21 June 2012; pp. 588–592.
29. Medaglia, C.M.; Serbanati, A. An Overview of Privacy and Security Issues in the Internet of Things. In The Internet of Things; Springer: New York, NY, USA, 2010; pp.389–395.
30. Sarvy, O.; Vacheraand, F. Security and Privacy Protection of Contac less Devices. In The Internet of Things; Springer: New York, NY, USA, 2010; pp. 409–418.
31. Liu, Y.; Peng, Y.; Wang, B.; Bai, X.; Yuan, X.; Li, G. The Internet of Things Security Architecture Based IBE Integration with the PKI/CA. In Proceedings of the Advanced Science and Technology Letters, Harbin, China, 18–20 April 2013; pp. 243–246.
32. Antonio, F.S.; Ramos Jose, L.H., Moreno, M.V. A decentralized approach for Security and Privacy challenges in the Internet of Things. In Proceedings of the IEEE World Forum on Internet of Things, Seoul, Korea, 6–8 March 2014; pp. 67–72.
33. Xiao, Y.; Li, C.-C.; Lei, M.; Vrbsky, S.V. Differentiated virtual passwords, secret little functions, and codebooks for protecting users from password theft. IEEE Syst. J. 2012, doi:10.1109/ JSYST.2012.2183755.
34. Asadpour, M.; Sattarzadeh, B.; Movaghar, A. Anonymous authentication protocol for GSM networks. Int. J. Secur. Netw. 2008, 3, 54–62.
35. Krontiris, I.; Dimitriou, T. Scatter–secure code authentication for efficient reprogramming in wireless sensor networks. Int. J. Sens. Netw. 2011, 10, 14–24.
36. Lin, X.; Ling, X.; Zhu, H.; Ho, P.; Shen, X. A novel localized authentication scheme in IEEE 802.11 based Wireless Mesh Networks. Int. J. Secur. Netw. 2008, 3, 122–132.
37. Kim, K.; Jeon, J.; Yoo, K. Efficient and secure password authentication schemes for low-power devices. Int. J. Secur. Netw. 2006, 2, 77–81.
38. Scannell, A.; Varshavsky, A.; LaMarca, A.; de Lara, E. Proximity-based authentication of mobile devices. Int. J. Secur. Netw. 2009, 4, 4–16
39. McCune, J.M.; Perrig, A.; Reiter, M.K. Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication. Int. J. Secur. Netw. 2009, 4, 43–56.
40. Laur, S.; Pasini, S. User-aided data authentication. Int. J. Secur. Netw. 2009, 4, 69–86.
41. Lee, S.; Sivalingam, K.M. An efficient One-Time Password authentication

scheme using a smart card. Int. J. Secur. Netw. 2009, 4, 145–152.

42. Miao, J.; Wang, L. Rapid Identification Authentication Protocol for Mobile Nodes in Internet of Things with Privacy Protection. J. Netw. 2012, 7, 1099–1105.
43. Du, X.; Xiao, Y.; Mohsen, G. An effective key management scheme for heterogeneous sensor network. Ad Hoc Networks 2007, 1, 24–34.
44. Liang, Z.; Chao, H. Multimedia Traffic Security Architecture for the Internet of Things. IEEE Netw. 2011, 25, 35–40.
45. Zhao, H.V.; Lin, W.S.; Liu, K.J.R. A Case Study in Multimedia Fingerprinting: Behavior Modeling and Forensics for Multimedia Social Networks. IEEE Signal Proc. Mag. 2009, 26, 118–139.
46. Chen, M.; Gonzalez, S.; Zhang, Q.; Leung, M.V.C. Software Agent-based Intelligence for Code-centric RFID Systems. IEEE Intell. Syst. 2010, 25, 12–19.
47. Kundur, D.; Luh, W.; Okorafor, U.N.; Zourntos, T. Security and Privacy for Distributed Multimedia Sensor Networks. Proc. IEEE 2008, 96, 112–130.
48. Zhou, L.; Xiong, N.; Shu, L.; Vasilakos, A.; Yeo, S. Context-Aware Multimedia Service in Heterogeneous Networks. IEEE Intell. Syst. 2010, 25, 40–47.
49. Zhou, L.; Wang, X.; Tu, W.; Muntean, G.; Geller, B. Distributed Scheduling Scheme for Video Streaming over Multi-Channel Multi-Radio Multi-Hop Wireless Networks. IEEE J. Sel. Area. Commun. 2010, 28, 409–419.
50. Eskicioglu, A.M. Multimedia Security in Group Communications: Recent Progress in Key Management, Authentication, and Watermarking. Multimed. Syst. 2003, 9, 239–248.
51. Susanto, H.; Muhaya, F. Multimedia Information Security Architecture Framework. In Proceedings of the FutureTech, Busan, Korea, 21–23 May 2010.
52. Gao, D.; Guo, Y.J.; Cui, J.Q.; Hao, H.G.; Shi, H. A Communication Protocol of RFID Systems in Internet of Things. Int. J. Secur. Appl. 2012, 6, 91–102.
53. Martin, G. A Study of the Random Oracle Model. Ph.D. Thesis, University of California at Davis, California, CA, USA, 2008.
54. Alomair, B.; Clark, A.; Cuellar, J.; Poovendran, R. Scalable RFID systems: A privacy-preserving protocol with constant-time identification. In Proceedings of the International Conference on Dependable Systems and Networks, Chicago, IL, USA, 28 June–1 July 2010.
55. Ye, N.; Zhu, Y.; Wang, R.C.; Malekian, R.; Min, L.Q. An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things. Int. J. Appl. Math. Inf. Sci. 2014, 8, 1617–1624
56. Mahalle, P.N.; Prasad, N.R.; Prasad, R. Object Classification based Context Management for Identity Management in Internet of Things. Int. J. Comput. Appl. 2013, 63, 1–6.
57. Chao, M.H.; Hsu, C.M.; Miaou, G.S. A Data Hiding Technique with Authentication, Integration, and Confidentiality for Electronic Patient Records. IEEE Trans. Inf. Technol. Biomed. 2002, 6, 46–53.
58. Gu, Y.; Wu, W. Mutual authentication protocol based on tag ID number

updating for low-cost RFID. In Proceedings of the IEEE International Conference on Network Infrastructure and Digital Content, Beijing, China, 6–8 November 2009; pp. 548–551.

59. Pateriya, R.K.; Sharma, S. An Ultralightweight Mutual Authentication Protocol for Low Cost RFID Tags. Int. J. Comput. Appl. 2011, 25, 28–35