Developing a Safer Educational Environment that Preserves Users' Privacy

Sofia Sakka[1], Vasiliki Liagkou[1] and Chrysostomos Stylios[1,2]

[1] Department of Informatics and Telecommunications, University of Ioannina, Arta, 47100, Greece
[2] Industrial Systems Institute, Athena RC, 26504 Patra, Greece
s.sakka@uoi.gr (S.S.); liagkou@uoi.gr (V.L.); stylios@uoi.gr/stylios@isi.gr (C.S.)

Abstract. This study proposes an e-attendance system that improves students' safety and preserves user privacy and children's rights. The system provides an access control system that combines Radio Frequency Identification (RFID) technology and identity management schemes. This technique can be used to track student attendance while guaranteeing their privacy is maintained precisely. In contrast to current methods, this work prioritises security and privacy concerns. The suggested method incorporates the blockchain strategy and privacy attribute-based credentials (P-ABCs) for secure and controlled identity management. Notably, the system avoids using cameras or biometric data to allay privacy concerns. To further improve student safety, future improvements might incorporate GPS technology.

Keywords: RFID, P-ABCs, Security, Privacy, Education.

1 Introduction

1.1 Problem statement

Always, the safety of students is a major issue. On the one hand, parents want to be sure that the school is a safe environment for their children; on the other hand, teachers, having a great responsibility, need something to feel more confident about the safety of their students. The method used to record students' attendance is done manually by a student or teacher in charge at the beginning of each lesson. Although this method has been prevalent for many years, it does not assure the students are on the school grounds.

For example, a student could leave the school during the schedule. The recorded absence will protect the teacher from the charges but not the child's safety. Something more drastic is needed so the student cannot be absent without justification, and the teacher is informed in time for absences. Thus, integrating advanced technology in educational environments is paramount for enhancing students' safety and privacy.

Many security solutions provide a sustainable educational environment, proposing different e-attendance systems, such as [1–5]. Although these proposals aim to ensure

students' safety, most of them do not consider vulnerabilities or risks that may violate their privacy. The problem is that they are not concerned with who collects the critical data of students. For example, attacks on the network layer, such as Radio Frequency Identification (RFID) spoofing and cloning, where the attacker spoofs RFID signals, and copies data from a pre-existing RFID tag to another RFID tag, could cause data breaches. Consequently, this could lead to the disclosure of personal student data such as name and address. When we consider the aftermath from the disclosure of this information, including kidnapping situations, we realize the need of implementing security and privacy-preserving solutions.

In this work, we propose privacy-preserving technologies to build a trustworthy educational environment. To our knowledge, there isn't an attendance system for educational environments that fulfils the security and privacy aspects. To deal with security and privacy problems it is necessary to observe the flow and storage of information between the involved entities. We try to implement the P-ABCs (Privacy Attribute-based Credentials) in an RFID-based system, enabling students to authenticate themselves in a privacy-preserving manner, and the credentials are verifiable on the blockchain. The implementation of a distributed identity management scheme, such as in [6,7], enables users to keep control of their data, deciding who can access it and how it might be used, and providing improved protection. The whole procedure is based on the principles of GDPR (General Data Protection Regulation). The use of biometric data of students is not recommended since they are stored in a database or the use of cameras that may raise concerns of privacy violation.

1.2 Related work

According to the literature, many e-attendance systems have been proposed for educational systems. Fig.1 demonstrates the evolution of these systems in educational environments during the last years. Obviously, the downward trend over the last year is since we are still going through this year and not to the system performance decline.

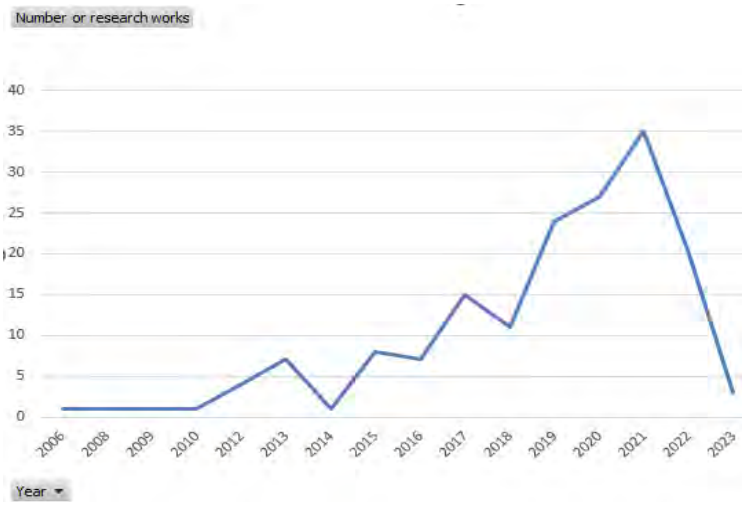

Fig.1: The evolution of e-attendances systems in educational environments during the last years

According to the research, we observed that the majority e-attendance systems for students were based on biometric or RFID authentication methods. In this work, we focus on RFID-based systems. Although many RFID-based attendance systems have been proposed in educational institutions, they focus on children's safety, but they do not mention the security and privacy of their private data. RFID systems have several security and privacy vulnerabilities, including tag cloning, eavesdropping/sniffing and replay attacks [8,9] .

Indeed, several RFID authentication protocols have been proposed, but most of them concern the health domain. In [10], four authentication schemes have been presented, based on the Elliptic Curve Cryptosystem (ECC) satisfying an interesting set of security features and being very efficient as they are proposed in the context of RFID.

In [10], a low-cost device serves as an RFID tag while our scheme uses a smartcard. This device is suitable for elliptic curve calculations, establishing a secure channel with the third trusted entity. On the contrary, the smart card is used for secure storage of sensitive information and executing cryptographic protocols. Generally, these schemes aim to establish a secure communication channel between the tag and the reader based on ECC, providing mutual authentication. and anonymity of the tag. However, the majority of the protocols, such as [11–13], that utilise the ECC to overcome the security flaws, have been proved that they are still vulnerable in threats, like impersonation attacks, tag cloning and location tracking attacks [14]. Especially, the scheme in [11] suffers from no integrity check and no scalability, [12] does not provide resistance against forward security and impersonation attacks, and [13] suffers from DoS, cloning, and location tracking attacks [14]. Apparently, the use of wireless broadcast channels for data transmission could lead to privacy leakage too. To ensure the security of the communication channels, protocols such as [15], utilise cloud-based techniques claiming to be robust against de-synchronisation, tag tracking, and replay attacks. However,

the authors in [16]showed that this scheme could not withstand the above threats. Also, approaches against RFID tag corruption, like the scheme in [17], include hardware primitives, such as Physical Unclonable Functions (PUFs). Nevertheless, this scheme does not support revocability and it is vulnerable to know session key attack.

Relevant research for educational environments [18] proposes using the Secure Multiparty Computation technique (SMC) by implementing Shamir Secret Sharing. However, this method requires too much hardware (especially RFID readers), and it is vulnerable to eavesdropping, cloning, and replay attack. To summarise, researchers have suggested several solutions, including encryption, authentication methods, pseudonymisation, and anti-sniffing techniques, to reduce security and privacy concerns.

2 The RFID-based attendance system

2.1 The system architecture

The basic idea is the usage of RFID, a technology that enables locating, real-time tracking, and identify objects or individuals using radio waves for developing a security system for students. The RFID consists of two components, the RFID tag and the RFID reader [19]. Every student must be equipped with a smart card that will serve as an RFID tag containing a unique identifier. On the other hand, the RFID reader acts as the gateway between the student and the information system of the school. The RFID reader will collect student information every time they enter or leave the school, counting how many students entered and sending information to the professor in case someone is absent. The students' smart card will not work for a third time a day, so he/she cannot leave the school without permission.

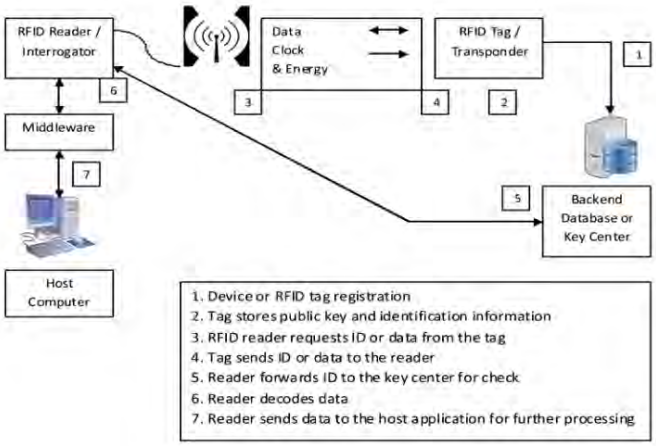

Fig.2: RFID main architecture [20]

Fig.2 indicates the basic operations in the RFID-based attendance system. The RFID Tag transmits its information to the Tag Reader (RFID Reader). The school's attendance system reacts to the RFID reader, which then transmits the response to the RFID

tag. Although the above scenario is quite simple and promises students' safety, it could violate students' privacy since it is not mentioned how the transmitted and collected data are protected. To solve this problem, we propose the implementation of distributed identity management scheme and privacy attribute-based credentials (P-ABCs) for secure and controlled identity management.

2.2 Challenges of an RFID-based system

RFID-based systems have a lot of potential, but they also have inherent challenges. To take full advantage of the RFID technology, while ensuring effective and safe operations, we should first recognize these challenges. According to [20], we present the key issues of RFID technology:

1. Tag/Reader Collision: Tag collision happens when several RFID tags are read at once, which causes data interference and decreased accuracy. It can be difficult to recognize and read individual tags in dense RFID environments, such as warehouses or retail stores, where many tags may be in the line of sight of a scanner. To address this problem, effective anti-collision algorithms and tag recognition methods must be used.
2. Reader-to-Tag Distance: The distance between the reader and the tag can affect the performance of RFID systems. The read range and accuracy can be influenced by elements like signal intensity, interference, and tag orientation. These characteristics must be carefully considered in order to ensure continuous and dependable communication between readers and tags, especially in dynamic environments.
3. Data Security and Privacy: RFID systems transmit sensitive data, such as students' information in our case. Unauthorized access to this data may lead to malicious or privacy-invading actions. Protecting the security and integrity of RFID data requires the implementation of strong encryption, authentication, and access control measures.
4. No uniform encoding: Tag information needs to be uniformly encoded to enhance information exchange. However, no consistent encoding standard for RFID tags has yet been created that is accepted globally.
5. Trust management scheme: Establishing trust management scheme in RFID systems between readers and tags as well as between readers and base stations is necessary to guarantee privacy. In this field, digital signature technology is frequently employed to prevent readers and tags from being counterfeited. The storage and computational resources needed by conventional cryptographic methods and protocols, which are utilized in digital signature technology, are far more than those of RFID tags. Therefore, the complexity of computational resources and storage issues must be considered in the RFID authentication technique.

2.3 Enhancing the security and privacy aspects

As mentioned previously, it is crucial to establish a trust management scheme to guarantee privacy aspects. P-ABCs allow for the selective sharing of validated attributes at the time of credential issue and provide a secure and reliable way to verify specific attributes without releasing personal information. In the distributed P-ABC credential approach, the user receives from the Identity Providers (IdPs) a set of credential fragments that he recomposes into a fully P-ABC credential. After that, the credential is stored locally in a secure way (e.g., smart card), and the user can generate privacy-preserving crypto-tokens to be presented to a relying party. The same obtained credential can be employed several times to derive unlikable tokens, and therefore, users do not need to be online to interact with the IdP to get the token. Thus, it enables face-to-face scenarios where the verifier relying party can be accessible by the user through short-range wireless communications (e.g., RFID Reader range), suitable for IoT, where the verifier, or even the user, might be impersonated by a smart IoT device.

Understanding the roles and interactions of these actors is essential for comprehending the overall system. So, we provide a concise overview introducing the key actors within our proposed system: The Attendance Verification System of the school performs access control by presenting a policy to the students. Only authorized users are given access to the Attendance Verification System, such as school personnel. The Attendance Certification system provides a web service to educational institutions where their personnel can be informed about student's' attendance record and may perform additional actions like uploading degrees. This information is then made available to the students and parents. School's Application Portal is a web base information portal through which the participating entities will get information about the pilot system and functionality as well as information about its usage. Moreover, this portal also contains the necessary links to the components of the system (i.e., School Certification System, Attendance Verification System). The School Certification System allows students to confirm their attendance status, or even graduates to prove degree possession. The Student's Home Application provides the student or parents with an interface that enables them to browse the credentials and create verification tokens if they want to share a medical certificate for justifying absence due to illness. Fig.3 indicates the above interactions:

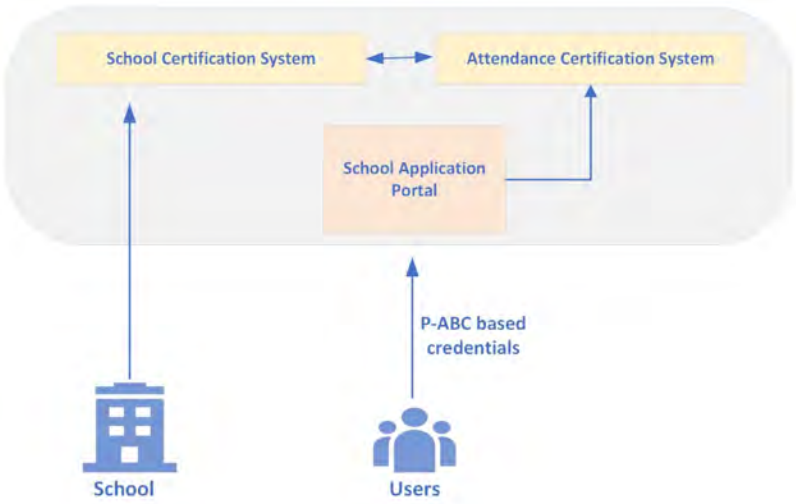

Fig.3: Overview of key actors in the proposed system

A cryptographic primitive that is typically being used when constructing ABC systems is the zero-knowledge proof of knowledge. It is a cryptographic protocol which allows a prover to convince a verifier that she knows a secret piece of information, without revealing anything more than what is already revealed by the statement itself [6,7]. However, issues, including poor usability and implementation difficulties, have prevented their acceptance in mainstream services. Additional issues include user accountability for securely keeping credentials and reliance on a single identity provider as a single point of failure. The distributed identity management on the blockchain serves as a privacy-preserving solution to these problems, preventing any authority from impersonating or tracking users by utilising distributed cryptography techniques and sharing the responsibility of the online Id-Provider among several authorities. This decentralised strategy of blockchain creates safe connections between users' physical and digital identities improving the integrity and privacy of the system. The proof-of-work feature of the blockchain protects the network and eliminates the need for a third party to validate and record transactions [21].

2.4 Developing a secure educational environment

We propose the use of the P-ABCs framework to manage the encrypted data that is transferred in the attendance system's database. The P-ABCs framework promises a trustworthy environment which ensures that student personal information is kept private, is not accessible, and is not subject to discrimination. At the time that the RFID Reader detects the student's smart card, it starts a communication link between the smart card and the school's attendance system. The purpose is to collect anonymously the student's attendance record, limiting access to only authorised individuals, like teachers and administrators.

The credentials are issued by the school to the students. The school may have to authenticate the students by requiring them to physically present themselves at the school's office. Then, a verifier must define which of the student's credentials are needed in order to be accepted by the system. The verifier's restrictions are described in its presentation policy, and a presentation token is created based on user's credentials including supporting cryptographic primitives. Thus, the school acts like an IDService Provider/Verifier and as an issuer. In addition, the school system should include a revocation authority who is responsible for revoking smart cards, i.e., when a student loses his smart card or graduates. Also, in such systems there is also a separate entity, the inspector, which is a trusted authority who can de-anonymize presentation tokens under specific circumstances [22]. In the context of privacy-preserving identity management, several other actors need to participate, such as parents and personnel for being informed about students' attendance record, and doctors for proving absence due to illness. The distributed privacy preserving protocol is applied during the above communication process, protecting the student's privacy, and ensuring authenticity. The interactions of these entities are illustrated in Fig. 4:

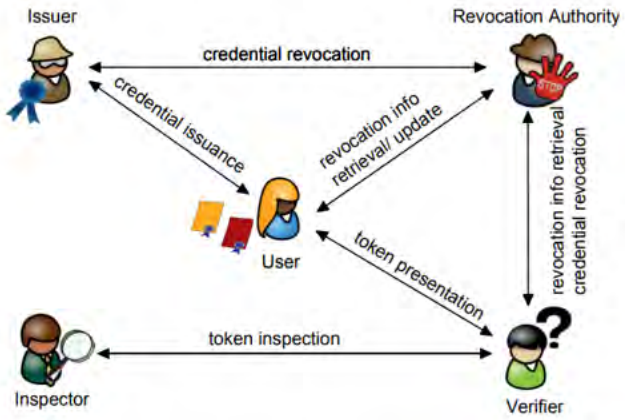

Fig. 4: Interactions of the entities [22]

When the students want to disclose a subset of attributes, such as their attendance information (unique identifier), they derive zero-knowledge proof of knowledge. This proof demonstrates that the user knows the digital signature on this attribute, while keeping the signature and the undisclosed attributes private. The service provider, such as the school's attendance system, receives the presentation token containing the zero-knowledge proof and the disclosed attributes. The service provider then verifies the validity of the zero-knowledge proof to ensure the user's authenticity and the integrity of the disclosed attributes. This verification process allows authorized individuals, like teachers and administrators, to access the necessary attendance information while preserving the privacy of the student's personal data.

The above procedures are merged into Fig 5. In the first step, each student is equipped with a smart card. The school initialises the smart card with the necessary information such as name, class, address, functioning as an RFID tag containing a

unique identifier. As mentioned, this step may also involve offline interactions, such as the student's physical presence in school for identity assurance purposes. This is a setup phase where the issuer (school) generates public issuer parameters and a secret issuance key. The issuer parameters are used by verifiers to authenticate the RFID tag. Thus, the school system establishes a secure and reliable identity for the student using the smartcard.

A counter is also implemented in the smart card for attendance measurement. The counter object includes parameters such as counter identifier, authentication key identifier, incremental index, threshold value, and a time-measuring variable. The school's system increments the counter associated with the student's identifier when the student waves their smart card to the RFID reader, indicating attendance [22]. More specifically, in step 2, the unique identifier of his smart card is being captured by the RFID Reader, and in step 3, this unique identifier which is actually a P-ABC token is sent to the school's attendance system. This token is the result of the signature in the zero-knowledge proof, to prove knowledge of the corresponding attributes without revealing any additional information. The counter that corresponds to this identifier of the smart card is increased by one unit. Finally, in step 4, the school's attendance system reacts to the RFID reader, which then transmits the response to the RFID tag, i.e., the student is informed that his request was valid. For detailed evaluation result, we refer to [23].

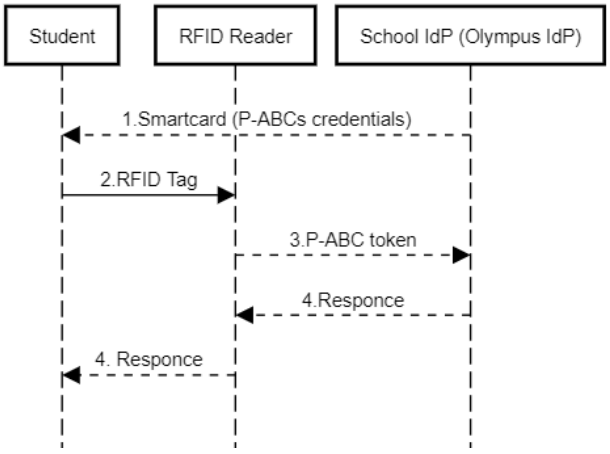

Fig 5: Basic operations of system's entities

Conclusion

This work has presented a trustworthy RFID-based e-attendance system implementing identity management schemes. It has introduced how the distributed identity management scheme can enhance the security and privacy aspects incorporated with P-ABCs for handling user's credentials. Intentionally, the system avoids authentication via biometric data considering that it is stored in a database. No biometric data encryption technologies are suitable for a system that concerns an educational environment

and must be frequent and efficient, in addition to the fact that it would be time-consuming for many students. Still, the use of cameras on school premises is not recommended because, in addition to the high cost, it may violate the privacy of school members. To further improve student safety, we envisage incorporating GPS technology in future work. This feature could be activated to locate the student in cases of emergency. However, we must consider that it requires the children to be equipped with GPS receivers or cellular phones, which could generate other problems.

Acknowledgements: This research work is co-funded by the project "Ecosystem for European Education Mobility as a Service:Model with Portal Demo (eMEDIATOR)" implemented under the Action "KA220-HED - Cooperation partnerships in higher education", funded by the Erasmus+.

References

1. Meghdadi, M.; Azar, A.A.; Meghdadi, M.; Azar, A.A. The Possibility of Using RFID System to Automate and Integrate the Attendance of Professors and Students in the Classroom. *Intelligent Control and Automation* **2016**, *7*, 93–109, doi:10.4236/ICA.2016.74010.
2. Okundamiya, M.S.; Emagbetere, J.; Edeko, F. Design and Implementation of a GSM Activated Automobile Demobilizer with Identification Capability. *Adv Mat Res* **2009**, *62–64*, 89–98, doi:10.4028/www.scientific.net/AMR.62-64.89.
3. Kirubanand, D.V.B. An Enhanced Biometric Attendance Monitoring System Using Queuing Petri Nets in Private Cloud Computing with Playfair Cipher. **2020**, doi:10.5373/jardcs/v12sp5/20201781.
4. Tamilselvan, S.; Ramesh, R.; Niveda, R.; Poonguzhali, P.; Dharani, S. IoT Based Touch-Free Attendance System (ITAS). *J Phys Conf Ser* **2021**, *1917*, null, doi:10.1088/1742-6596/1917/1/012012.
5. Htwe, K.M.; Htun, Z.M.M.; Tun, H. Design And Implementation Of Bank Locker Security System Based On Fingerprint Sensing Circuit And RFID Reader. *International Journal of Scientific & Technology Research* **2015**, *4*, 6–10.
6. Moreno, R.T.; Rodriguez, J.G.; Lopez, C.T.; Bernabe, J.B.; Skarmeta, A. OLYMPUS: A Distributed Privacy-Preserving Identity Management System. *GIoTS 2020 - Global Internet of Things Summit, Proceedings* **2020**, doi:10.1109/GIOTS49054.2020.9119663.
7. Bernabe, J.B.; García-Rodríguez, J.; Krenn, S.; Liagkou, V.; Skarmeta, A.; Torres, R. Privacy-Preserving Identity Management and Applications to Academic Degree Verification. *IFIP Adv Inf Commun Technol* **2022**, *644 IFIP*, 33–46, doi:10.1007/978-3-030-99100-5_4/FIGURES/4.
8. Burmester, M.; De Medeiros, B. RFID Security: Attacks, Countermeasures and Challenges.
9. Grover, A.; Berghel, H. A Survey of RFID Deployment and Security Issues. *Journal of Information Processing Systems* **2011**, *7*, doi:10.3745/JIPS.2011.7.4.561.
10. Lamrani Alaoui, H.; El Ghazi, A.; Zbakh, M.; Touhafi, A.; Braeken, A. A Highly Efficient ECC-Based Authentication Protocol for RFID. *J Sens* **2021**, *2021*, doi:10.1155/2021/8876766.

11. Jin, C.; Xu, C.; Zhang, X.; Li, F. A Secure ECC-Based RFID Mutual Authentication Protocol to Enhance Patient Medication Safety. *J Med Syst* **2016**, *40*, 1–6, doi:10.1007/S10916-015-0362-8.
12. Chou, J.S. An Efficient Mutual Authentication RFID Scheme Based on Elliptic Curve Cryptography. *Journal of Supercomputing* **2014**, *70*, 75–94, doi:10.1007/S11227-013-1073-X/TABLES/2.
13. Shen, H.; Shen, J.; Khan, M.K.; Lee, J.H. Efficient RFID Authentication Using Elliptic Curve Cryptography for the Internet of Things. *Wirel Pers Commun* **2017**, *96*, 5253–5266, doi:10.1007/S11277-016-3739-1/TABLES/3.
14. Shariq, M.; Singh, K.; Bajuri, M.Y.; Pantelous, A.A.; Ahmadian, A.; Salimi, M. A Secure and Reliable RFID Authentication Protocol Using Digital Schnorr Cryptosystem for IoT-Enabled Healthcare in COVID-19 Scenario. *Sustain Cities Soc* **2021**, *75*, 103354, doi:10.1016/J.SCS.2021.103354.
15. Fan, K.; Luo, Q.; Zhang, K.; Yang, Y. Cloud-Based Lightweight Secure RFID Mutual Authentication Protocol in IoT. *Inf Sci (N Y)* **2020**, *527*, 329–340, doi:10.1016/J.INS.2019.08.006.
16. Adeli, M.; Bagheri, N.; Sadeghi, S.; Kumari, S. Xperbp: A Cloud-Based Lightweight Mutual Authentication Protocol.
17. Xu, H.; Chen, X.; Zhu, F.; Li, P. A Novel Security Authentication Protocol Based on Physical Unclonable Function for RFID Healthcare Systems. *Wirel Commun Mob Comput* **2021**, *2021*, doi:10.1155/2021/8844178.
18. Putrada, A.G.; Abdurohman, M. Increasing the Security of RFID-Based Classroom Attendance System with Shamir Secret Share. *International Journal on Information and Communication Technology (IJoICT)* **2020**, *6*, doi:10.21108/ijoict.2020.61.480.
19. Roberts, C.M. Radio Frequency Identification (RFID). *Comput Secur* **2006**, *25*, doi:10.1016/j.cose.2005.12.003.
20. Gupta, B.B.; Quamara, M. An Overview of Internet of Things (IoT): Architectural Aspects, Challenges, and Protocols. *Concurr Comput* **2020**, *32*, doi:10.1002/CPE.4946.
21. Ali, O.; Jaradat, A.; Kulakli, A.; Abuhalimeh, A. A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities. *IEEE Access* **2021**, *9*, 12730–12749, doi:10.1109/ACCESS.2021.3050241.
22. Rannenberg, K.; Camenisch, J.; Sabouri, A. Attribute-Based Credentials for Trust: Identity in the Information Society. *Attribute-Based Credentials for Trust: Identity in the Information Society* **2015**, 1–391, doi:10.1007/978-3-319-14439-9/COVER.
23. Stamatiou, Y.; Benenson, Z.; Girard, A.; Krontiris, I.; Liagkou, V.; Pyrgelis, A.; Tesfay, W. Course Evaluation in Higher Education: The Patras Pilot of ABC4trust. In *Attribute-Based Credentials for Trust: Identity in the Information Society*; 2015.