Secure Web Application Development Using Digital Signature

1. Abstract

In the present-day world, where online education is of utmost importance, many organizations offer certificates to the participants for future references. Many people, who have not achieved any of these certificates, often spoof the certificates received by other participants for academic gain. Such instances degrade the value of said certificates and the participants who worked hard to achieve these accomplishments are unable to harvest the benefits. These certificates often lose their credibility in the industry. Hence, a system has been proposed where organizations can issue certificates, whose validity can be confirmed by an automated system, wherein multiple layers of hashing and encryption help in creating a custom protection system to avoid any kind of spoofing. Usage of hashing along with encryptions makes sure no reverse-engineered attacks can be used to spoof the certificates while encryption using private keys ensure that duplicate certificates cannot be generated.

Keywords: Encryption, hashing, digital signature, digital certificate

2.Introduction

In the modern-day recruitments, a lot of emphasis is given to the certificates achieved by completing certain online courses and achieving particular grades in some examinations. Such certificates, received from industry recognized organizations such as NPTEL, ISACA etc. are a token of an applicant's calibre in a given field. These certificates are taken into account while shortlisting candidates for University admissions, Job recruitments, Promotions etc.

But not all are able to achieve these certificates. In many such cases, the candidates often spoof the certificates in order to achieve academic or monetary gains. Such incidents lead to degradation in value of certificates achieved by hard working and capable candidates and gives the candidates who spoofed the certificates, unfair advantages in these processes.

In order to tackle this, this paper proposes a digital certificate generation system, where certificates are generated along with digital signatures and unique tokens generated with multiple layers of hashing and

encryption (using static as well as dynamic private keys) and one can easily check the validity of a certificate using an automated system.

The structure of the paper is as follows: Section 2, Literature survey- discusses related work done by previous authors. Section 3, Proposed work, describes the modules used in the project and explains the environment setup.. In section 4, our methodology is being explained. Section 5 discusses the attack generation. Section 6 discusses attack detection and prevention. Following that, in Section 7, Results have been displayed. Section 8 discusses conclusion and future work.

3. Literature Review

Tons of certificates were being forged and to get a solution, the use of blockchain was used to overcome this problem. The generation of hash and QR code was used to secure the certificate.This was used to reduce the risks of the certificate being misused[1] Authentication of IOT devices on the network required port knocking with port scanning.Port knocking approaches when carried out alone suffers from security issues. This paper aims at fixing the existing port knocking methods to authenticate among the internet of things devices[2]

The use of x.509 Check tool is designed to test the quality of the digital certificates.It provides a deep analysis and configuration of the certificate.The use of this tool is helpful foe everyone having original certificates and they want to safeguard it.A report has been generated with this tool. The existence of issues and a lot of problems related to security can be resolved using this tool. [3] A major issue faced by educational institutes is forgery of certificates., the certificates are secured using blockchain with smart contracts. Blockchain prevents the certificate from being manipulated and helps in implementing

a verification system.It gives a quick response code when a certificate is used. A watermark is used to showcase the authentication.[4]

While emailing clients, a lot of the documents gets forged and go missing and they are tampered with. The use of an identity based encryption, which is an asymmetric cryptographic algorithm us put to use where the public keys and the users unique keys are kept separately and in safe distance from the malicious users.They are also making use of the RSA algorithm to with thunderbird and outlook for better UI and better security reasons. [5]

In the present day situation, banking is losing its high security and a lot of forgery has been taking place. Its been resulting in loss of economy, robbery and unwanted and high transactions. To save these, asymmetric encryption techniques and RSA algorithm was made use of to improve the core of the IP core.[6] As mentioned above, in situations where in banking sectors strong security is of extreme importance, algorithms such as DSA and RSA are used together. They have generated public and private key.The system verifies it using an OTP to confirm the authentication. [7]

This system was specifically designed for the Brazilian government for information kept getting leaked and forged. Thats when the government had decided to come up with the digital signature. This work had depicted digital signature which was used to save the situation the government was stuck in.It have a safer, securer and faster way of signing documents. [8] Digital certificates were the safest way of securing documents. They made use of cryptographic methods to explore various aspects of data security. Algorithms such as ECC, Rivest, Shamir and RSA were used. The parameters were encrypted and decrypted. Both the public and the private sector made use of this system to stop duplicates from being formed.[9]

To secure certificates, they used peer to peer network and blockchain to prevent the deception of certificates and it was validated using blockchain. They were able to prevent the certificated from being forged and used a quick response code.The authenticity of the certificate was improved using the quick response code by also adding a watermark. [10] Previous blockchain had papers which were still not enough to save the sensitive information on the documents. They combined blockchain along with certificate based technologies. They used high efficiency networks which was used to identify participants who forge documents[11]

In this paper, they used hash code and blockchain technology to provide a more secure system. They used digital certificates in educational institutes so that its less tedious and cumbersome. Hence, they resorted to securing it using these methods.[12] In smart cities where everything is getting secured,

people are finding ways to forge it. Edge computing infrastructure along with authentication schemes are helpful to secure the safe grid environment. They used DRMAS to provide the necessary security to safeguard the system.[13]

The secure socket layer is used for verifying the certificate in IOT Applications which is helpful in preventing it from getting exploited by the man in the middle attack and TLS attacks. In this paper, they made use of IotVerif helpful in reverse engineering in IOT for their messaging protocols and to identify vulnerabilities. [14] For securing communication between parties, they have made use of the elliptic-curve Qu-Vanstone (ECQV) implicit certificate has been employed for lightweight security association establishment for the IoT environment. [15]

Certificate Revocation Guard was used to check if the certificate had minimising bandwidth, latency or storage whole revocation. They had installed CRG on ISP level.It decreases the bandwidth overhead and network latencies by 95%.[16] In this paper, the certificates are used to modify the nominal trajectory in a minimally invasive way to avoid collisions. The proposed collision avoidance strategy complements existing flight control and planning algorithms by providing trajectory modifications with provable safety guarantees. [17]

Without security, VANET is exposed to several threats, among which one of the threat is Sybil attack. One of the robust secure mechanism adopted is a cryptographic digital signature used to establish the faith between the various participating entities.[18] A certificate validation system that can effectively handle certificate validation during TLS handshakes. The system utilizes Internet service providers (ISPs) as the primary entity for certificate validation exploiting the fact that any Internet access request must pass through the ISP proxy-cache servers. [19]

This article presents the technical details of the Extensible Authentication Protocol (EAP) and IEEE 802.1x by using WIRE1x, an open-source implementation of IEEE 802.1x client (supplicant) and various EAP-based authentication mechanisms. By using a real implementation, 802.1x and EAP should be easily understood.[20]

4.Proposed work

In the previous section about the related work, conclusions have been drawn about how this project is different from the ones already done.

Firstly, the system lets the users choose his choice of template of certificate. It is then his wish to choose where his text can go given the csv and its headers. The certificate is encrypted and decrypted, it also

has a digital signature. Generally, this is where the existing work in this domain ends. But this system has also created a verification link which takes user to the website where the original certificate is present. So ,even if someone tampers with the details inside the certificate, it will not be reflected in the verification link and it will be immediately seen.

4.1. The modules used in our project:

4.1.1. MongoDB

It is the most widely used NoSQL database available with both cloud database as well as local database functionalities. For the purpose of this project, the usage of cloud based database is done. It contains fields or name-value pairs. Collections store groups of documents and functions. They are equivalent to relational database tables.

It is one of the numerous nonrelational database technologies which arose in the mid-2000s under the NoSQL banner for use in big data applications and other processing jobs involving data that doesn't fit well in a rigid relational model. Instead of using tables and rows as in relational databases, the MongoDB architecture is made up of collections and documents.

4.1.2. NodeJS

It is the most prevalent backend framework being used in the full-stack industry. It provides a very comfortable approach towards developing restful APIs. Hence the same backend can be used to develop Web, Desktop and Mobile applications. Node.js uses an event-driven, non-blocking I/O model that makes it translucent and productive and efficient. Node.js makes developing such tools highly facile with the open source subdivision and a special package manager.
It was easier for developers to grasp on Node.js and leverage from their JavaScript skills and so they no longer needed to work in different front-end and back-end teams as they could now be combined into a single functional unit and focus more on application development than firefighting.

4.1.3. ReactJS

It is one of the modern JS front-end frameworks, developed and maintained by FACEBOOK. It helps create dynamic and component based interactive User Experience.

React.JS is an open source JavaScript library which is used for building user interfaces particularly for single page applications. React JS used for handling view layer for web and mobile apps. React JS allow user to create reusable UI components.

React Js was first created by Jordan Walke, Jordan Walke is a software engineer working for Facebook. React JS was first used in Facebook's newsfeed in 2011 and on Instagram.com in 2012.

4.2. Environment setup:

This system can be set up on any Windows-based operating system machine. The steps to Setup are as follow:

1. Download and install NodeJS LTS version from https://nodejs.org/en/download /
2. Clone our repository from https://github.com/nkartik01/isaa_backend.git
3. Navigate to repository folder and run the following commands:
4. npm install
5. npm run server
6. This will start the server at port 5000. The project is now working.

4.3. Methodology

The Following is our encryption system as shown in Figure1:

1. The project is being implemented with front-end and back-end running on different server ports, making all our processing happen in the backend server, securing our logic and preventing any exploitation of the system.
2. Front-end user has to login into the website in order to use the certificate creating features, as all requests made in this process from front-end to backend will require access tokens, without which the services will not work. The token is a private key based encrypted JSON object, containing the user's unique id.
3. User will upload an CSV file with the first row considered as field names, where ‘email’ as a field must be present, along with an image of the required certificate template. The user will be prompted to mark positions, where the user wants to print the details in the certificate.
4. These details will then be sent to the backend where the csv will be read and details will be read from the csv file and inserted at concerned positions in the certificate.
5. This generated certificate will then be inserted into a pdf file and an unique id will be issued to the particular certificate. This ID is stored in the database along with an encryption-hashing token, generated by a process of dual dynamic + static private key encryption and multiple layers of hashing of data taken from the csv file.
6. The generated PDF is then digitally signed and mailed to the respective mail IDs.

Architecture Diagram

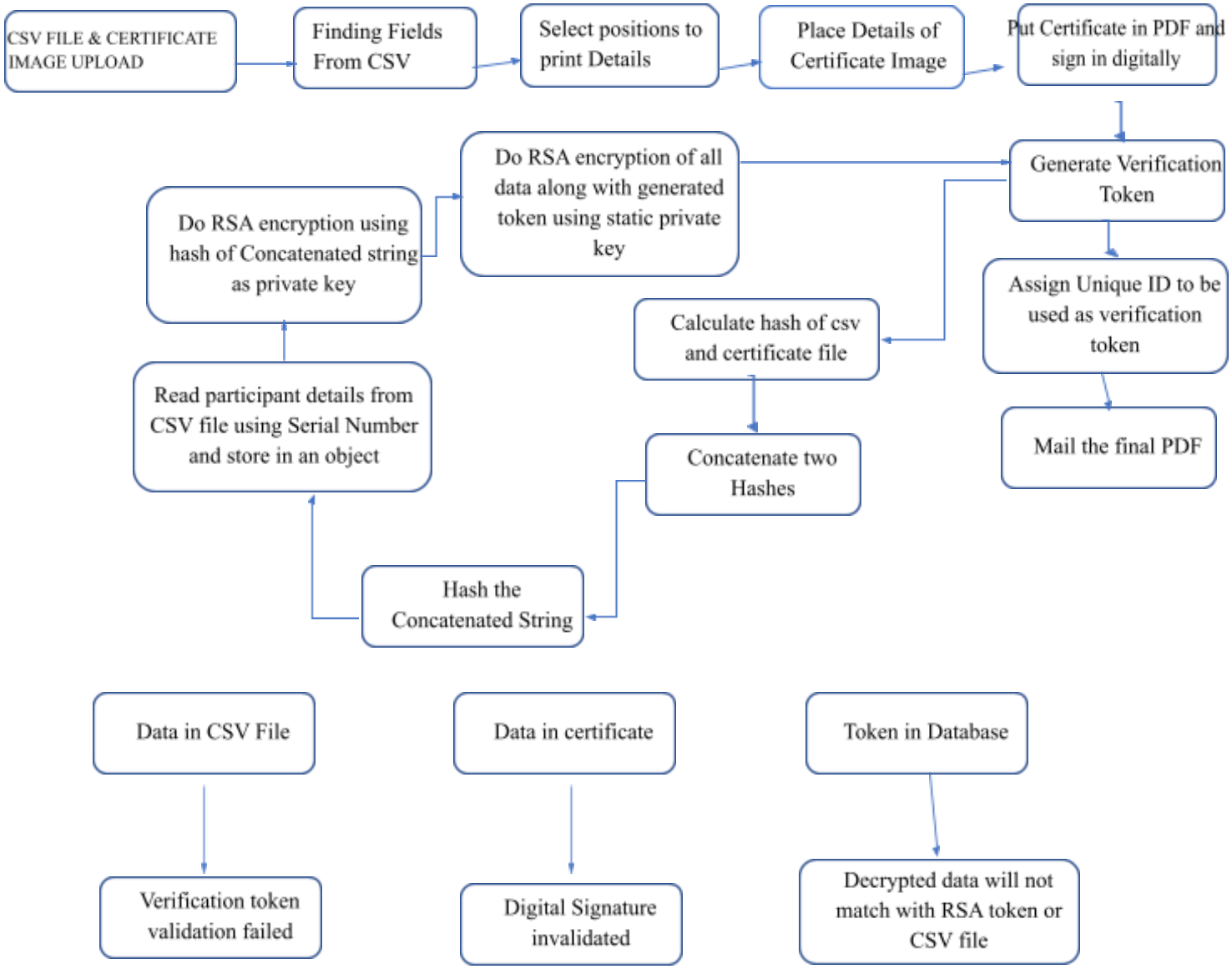

Figure1: The Attack Generation and Detection Architecture

4.4. Attack Generation:

After careful analysis and research, we identified that generally there exists some common patterns, features. We shed light on the important feature such as change of verification link, spoofing of PDF, spoofing of NoSQL database and spoofing stored CSV files

4.5. Attack Detection and prevention:

For verification of certificate using verification link, the corresponding token is accessed from the database. It is decoded along the static private key, the details thus revealed about csv file id and serial number are again retrieved and matched with verification token. If details match, the data is then processed in order to regenerate the certificate, which is then displayed in the front end.

Algorithm:

- Calculate the Hash of certificate and CSV file.
- Concatenate the two hashes.
- Hash the concatenated string.
- Read participant details from CSV file and serial number and put all in the object.
- Do RSA Encryption using a hash of concatenated string as the private key.
- Do RSA Encryption of All Data Along with generated token using a static private key.

4.6 Attack Generation and Detection Architecture

1.Edit certificate: This will be handled by the digital signature added to the certificate, as any changes to the certificate file will invalidate the certificate.

2.Morph Database: This is a far-fetched case, as we use highly protected cloud database, one could possibly get into the database and change the data associated with the certificate, but this will not be beneficial, as the data present in database has been processed through multiple layers of hashing and encryption, both Symmetric as well as Asymmetric.

3. Change the files stored in the server:This again is an unlikely scenario, but nonetheless, if it happens, the database token will not match with the storage file's values, and hence we will know that the record has been tampered with.

6.Results and Discussions:

The main purpose of this project is to present a system that can be used in many institutions for generating and verifying a certificate as shown in Figure2. It is achieved by designing a website which takes in certificate template image, participants details, and asking the certificate issuer to mark the places where information is to be printed. An automated system then generates encrypted tokens, verification link and certificates and mail a digitally signed certificate to the participant.

The encrypted token, verification link and input files are all interlinked to each other, hence any discrepancy in even any one of them is enough to let the system know that there have been manual modifications to the data and hence the spoofed certificates are not verified.

As discussed in Table1, this system is able to stop any kind of spoofing to disrupt the integrity of the certificate issuing authority and the certificate itself and provide a foolproof system to issue safe certificates digitally.

Figure2: The certificate is being displayed from the mail

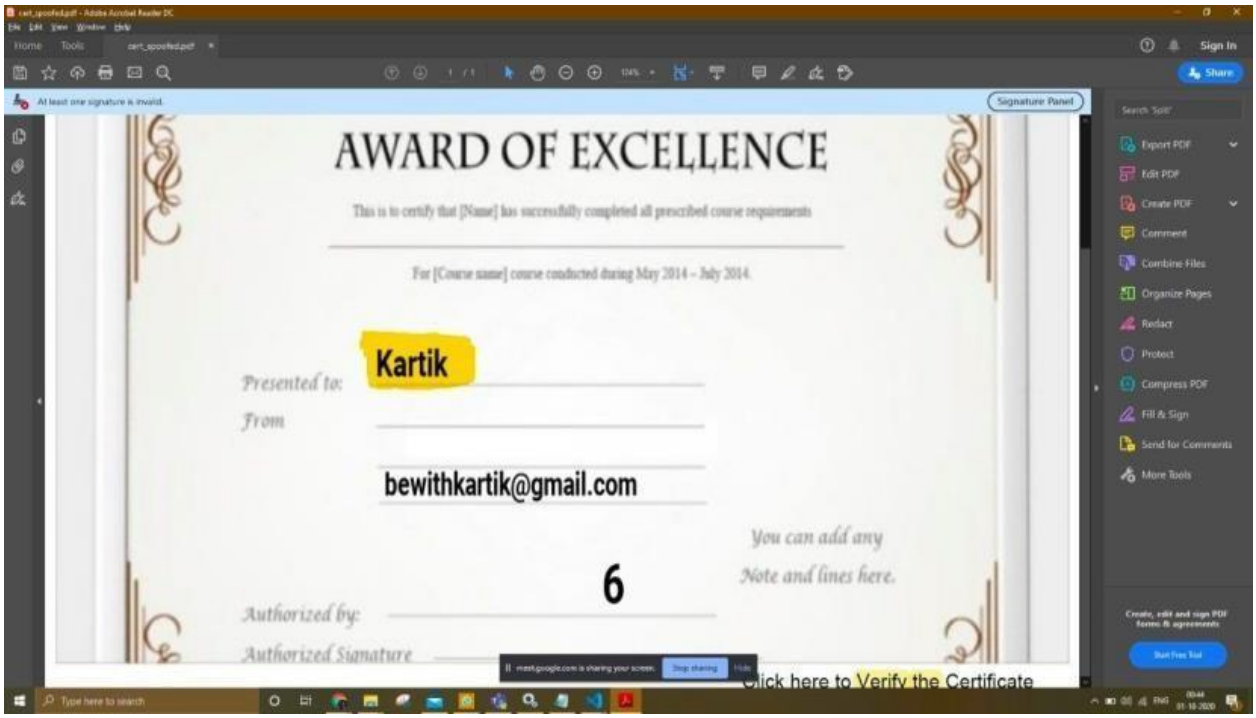

Figure3: Proof that that the link is bogus

Table 1: State of system before and after prevention techniques

Before encryption	After encryption
Verification link was changed successfully.	Certificate was not found as the link was not valid anymore
PDF was spoofed successfully and was not known to the outside world.	The authenticity of the certificate changed and the user was caught in changing details of the certificate.
No SQL Database got manipulated. The integrity of the certificate was trying to be tampered.	Because of strong encrypt, the accessing of the database and spoofing wasnt possible.
Trying to manipulate the content of the csv.	A warning was displayed that the certificate was bogus/tampered with.

7. Conclusion and future work: We were able to design and implement a system to generate digital certificates from a list provided in a .csv file and map its content on a certificate template, provided by the user and the individual certificates to the email ids provided in the .csv file corresponding to each participant. We were able to manage all of the above process in an automated manner. We also issued unique verification links along with each certificate that could be used to verify the validity of each certificate individually and find out if any of the information associated with these certificates were tampered with or not. In future, we wish to be able to identify at which level the spoofing has occurred, and hence over-write the spoofed sections with correct information, in-order to restore stability in the system. We also plan to introduce QR Codes as a method to verify the certificate as it has emerged as a prevalent method of accessing links.

References:

[1]J. Cheng, N. Lee, C. Chi and Y. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455.6.

[2]B. Mahbooba and M. Schukat, "Digital certificate-based port knocking for connected embedded systems," 2017 28th Irish Signals and Systems Conference (ISSC), Killarney, 2017, pp. 1-5, doi: 10.1109/ISSC.2017.7983645.

[3]A. Alrawais, A. Alhothaily and X. Cheng, "X.509 Check: A Tool to Check the Safety and Security of Digital Certificates," 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI), Beijing, 2015, pp. 130-133, doi: 10.1109/IIKI.2015.36.

[4]R. Poorni, M. Lakshmanan and S. Bhuvaneswari, "DIGICERT: A Secured Digital Certificate Application using Blockchain through Smart Contracts," 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2019, pp. 215-219, doi: 10.1109/ICCES45898.2019.9002576.

[5]J. Wu, Y. Long, Q. Huang and W. Wang, "Design and Application of IBE Email Encryption Based on Pseudo RSA Certificate," 2016 12th International Conference on Computational Intelligence and Security (CIS), Wuxi, 2016, pp. 282-286, doi: 10.1109/CIS.2016.0071.

[6]Liu B. (2020) Research and Implementation of RSA IP Core Based on FPGA. In: Huang C., Chan YW., Yen N. (eds) Data Processing Techniques and Applications for Cyber-Physical Systems (DPTA 2019). Advances in Intelligent Systems and Computing, vol 1088. Springer, Singapore. https://doi.org/10.1007/978-981-15-1468-5_154

[7]Ashiqul Islam M., Kobita A.A., Sagar Hossen M., Rumi L.S., Karim R., Tabassum T. (2021) Data Security System for A Bank Based on Two Different Asymmetric Algorithms Cryptography. In: Suma V., Bouhmala N., Wang H. (eds) Evolutionary Computing and Mobile Sustainable Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 53. Springer, Singapore. https://doi.org/10.1007/978-981-15-5258-8_77

[8]Ribeiro R.C., Canedo E.D. (2020) Digital Signature in the XAdES Standard as a REST Service. In: Gervasi O. et al. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science, vol 12249. Springer, Cham. https://doi.org/10.1007/978-3-030-58799-4_49

[9]Akshaya B., Rajendiran M. (2020) Automatic Inspection Verification Using Digital Certificate. In: Hemanth D., Kumar V., Malathi S., Castillo O., Patrut B. (eds) Emerging Trends in Computing and Expert Technology. COMET 2019. Lecture Notes on Data Engineering and Communications Technologies, vol 35. Springer, Cham. https://doi.org/10.1007/978-3-030-32150-5_83

[10]R. Poorni, M. Lakshmanan and S. Bhuvaneswari, "DIGICERT: A Secured Digital Certificate Application using Blockchain through Smart Contracts," 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2019, pp. 215-219, doi: 10.1109/ICCES45898.2019.9002576.

[11]B. Liu, L. Xiao, J. Long, M. Tang and O. Hosam, "Secure Digital Certificate-Based Data Access Control Scheme in Blockchain," in IEEE Access, vol. 8, pp. 91751-91760, 2020, doi: 10.1109/ACCESS.2020.2993921.

[12] A. Gayathiri, J. Jayachitra and S. Matilda, "Certificate validation using blockchain," 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2020, pp. 1-4, doi: 10.1109/ICSSS49621.2020.9201988.

[13]S. A. Chaudhry, H. Alhakami, A. Baz and F. Al-Turjman, "Securing Demand Response

Management: A Certificate-Based Access Control in Smart Grid Edge Computing Infrastructure," in IEEE Access, vol. 8, pp. 101235-101243, 2020, doi: 10.1109/ACCESS.2020.2996093.

[14]A. Liu, A. Alqazzaz, H. Ming and B. Dharmalingam, "IoTVerif: Automatic Verification of SSL/TLS Certificate for IoT Applications," in IEEE Access, doi: 10.1109/ACCESS.2019.2961918.

[15]C. Park, "A Secure and Efficient ECQV Implicit Certificate Issuance Protocol for the Internet of Things Applications," in IEEE Sensors Journal, vol. 17, no. 7, pp. 2215-2223, 1 April1, 2017, doi: 10.1109/JSEN.2016.2625821.

[16]Q. Hu, M. R. Asghar and N. Brownlee, "Certificate Revocation Guard (CRG): An Efficient Mechanism for Checking Certificate Revocation," 2016 IEEE 41st Conference on Local Computer Networks (LCN), Dubai, 2016, pp. 527-530, doi: 10.1109/LCN.2016.84.

[17]L. Wang, A. D. Ames and M. Egerstedt, "Safe certificate-based maneuvers for teams of quadrotors using differential flatness," 2017 IEEE International Conference on Robotics and Automation (ICRA), Singapore, 2017, pp. 3293-3298, doi: 10.1109/ICRA.2017.7989375.

[18]D. S. Reddy, V. Bapuji, A. Govardhan and S. S. V. N. Sarma, "Sybil attack detection technique using session key certificate in vehicular ad hoc networks," 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), Chennai, 2017, pp. 1-5, doi: 10.1109/ICAMMAET.2017.8186733.

[19]A. Alrawais, A. Alhothaily, X. Cheng, C. Hu and J. Yu, "SecureGuard: A Certificate Validation System in Public Key Infrastructure," in IEEE Transactions on Vehicular Technology, vol. 67, no. 6, pp. 5399-5408, June 2018, doi: 10.1109/TVT.2018.2805700.

[20]Jyh-Cheng Chen and Yu-Ping Wang, "Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience," in IEEE Communications Magazine, vol. 43, no. 12, pp. supl.26-supl.32, Dec. 2005, doi: 10.1109/MCOM.2005.1561920.