BOHR

BOHR International Journal of Smart Computing and Information Technology
2021, Vol. 2, No. 1, pp. 53–58
DOI: 10.54646/bijscit.2021.19
www.bohrpub.com

METHODS

An improved public key infrastructure-based digital signature authentication service for higher key storage system

B. Gopi* **and M. Suthársan**

Department of ECE, Muthayammal Engineering College, Namakkal, India

***Correspondence:**
B. Gopi,
profgopib@gmail.com

Received: 15 August 2021; **Accepted:** 02 September 2021; **Published:** 11 October 2021

In general, we quickly forget about boxes with paper archives, and there is not even a single sheet of paper on the desktop. If a paper document is sent to the institution through regular mail, the artifact is immediately scanned and digitized. In fact, it turned out to be quite the opposite. The more a company uses computers for digital workflows, the more it documents and prints. Above all, every document must be authenticated. A document without a signature is only a draft or an information note. To get the signature, the documents are printed and then often scanned, and the original documents are kept on file. It is now clear that the (paperless) workflow cannot be implemented without electronic digital signatures. In this study, an improved public key infrastructure-based Digital Signature Authentication Service is proposed for higher key storage system. In this method, the CAs included in the list provide certificate-based digital identifiers and time stamping services that comply with global regulations, such as the eIDAS standard. Electronic digital signatures are already supported for most popular office document formats. Timestamps are supported, including multi-person document signatures.

Keywords: digitized, digital, authenticated, signature, information, paperless, Public-key, certificate

Introduction

The Digital Signature Service (DSS) is a scalable application programming interface (API)-enabled platform for rapidly deploying digital signatures (1, 2). For your own DSS service, you need to set up more than just sign-on workflows and user management (3). Signing certificates are required to verify the identity of the author of each document (4). These include cryptographic components such as key management, a FIPS level 2 or higher key storage system (HKSS) (such as hardware tokens or hardware security module [HSM]), an OCSP or CRL service, and a timestamp service (5–7). Integrating these components, especially for direct integration with the HSM, whether in the cloud or on premise, requires significant effort from IT and security departments, good cryptography knowledge, and the availability of necessary resources (8–10). When evaluating digital signature solutions, it is important to consider these hidden costs, investments, limitations, and overheads. Individually, if the DSS service is critical to the organization, it should operate with high levels of uptime and provide high performance (11, 12). That means you should design your solution with a certain amount of redundancy – with margin for the future (13). Consider that business is characterized by growth. Infrastructure must be scalable (14).

- Paperless workflow: Saves time, money, and resources (15).
- Effective business processes: Electronic signing makes every transaction a smooth process (16).
- Mobile capabilities: It becomes easier to communicate with the company and customers (17).

Ultimately, each organization must decide which DSS option best suits their project requirements (18). It takes into account the requirements of regulatory bodies, the size of the organization, and other factors, often unique to each case (19, 20). An electronic signature (ES), a digital document signed by ES, is equivalent to a paper document with a handwritten autograph (21, 22). A ”cloud” ES has all the characteristics of a regular one; it is not stored on a flash drive or computer, but on the Internet – on a special, secure server, in the “cloud” (23, 24). The signing and encryption of the document also take place there; therefore, such an ES does not require the installation of special software on the computer (25–27). One of the advantages of the "cloud" signature is the ability to sign documents (including reports) and send them from any device anywhere in the world (28).

An ES “in the cloud” is something many of us use every day without even realizing it (29). The most notable example is the authentication mechanism in mobile and Internet banks, after entering the password, a one-time pin code is sent to you via SMS (30). Such two-level authentication, in essence, can already be an ES (31). With the help of ES, companies can submit reports to tax and other regulatory authorities (32), submit and recall that they conduct electronic document management. Digital signature is also widely used in public procurement (33). The technology of “cloud” ES, which appeared several years ago, makes this tool accessible to businesses (34). This is confirmed by tens of thousands of customers. One has to imagine a situation where a forwarding driver gets on a plane not with a wad of paper but with a tablet (35). At the point of shipment, he signs a bill of lading with the customer (36). But the “cloud” ES brings the main advantage when the delivery document differs from the quantity of goods actually sent (resorting to breakage during transport) (37).

Related works

ES performs the same function as a stamped signature. It ensures the authenticity of the document and contains the private and public keys (38). The document is signed using a private key, which is usually stored on a special medium – a token. You can buy a service from many companies that provide such services, except for the availability of a standard set of documents; no special requirements are required (39). “Cloud” ES is a regular ES, but with a difference: the private key is stored on the servers of the certificate authority, and the signing of documents is carried out there (40). The signer’s identity is usually verified by sending an SMS to a mobile phone. The technology is based on a special ES server located in the “Cloud” (41). For example, if a user needs to send a report to the tax office, his accounting system communicates with the ES server and sends him a document to sign (42). The ES server is obliged to request permission from the user – this can be done by sending a transaction confirmation code to his mobile phone, similar to Internet banking (43). By entering the confirmation code in the system, the user authorizes access to the ES key, and a signature is created for the document (44). All ES keys are stored in encrypted form on a special device that meets the most stringent security requirements (45). The operator of the ES server shall take all measures to minimize the risk of unauthorized access to the keys (46).

To use a “classic” ES, you need to purchase a token and special software. This is a significant expense, especially for start-up entrepreneurs (47). This software needs to be installed and configured if you are going to use the signature on multiple workstations – separately for each location (48). A ”cloud” ES does not require the purchase of software or pre-configuration and cannot be lost or forgotten. Unlike traditional technologies, “Cloud” ES is available to users on any operating system and platform, including mobile devices (49). “Cloud” ES is popular among small companies or individual entrepreneurs who actively use services such as “online accounting and online document management” (50). In large companies that do not use “clouds,” using such a signature may be more expensive and difficult than using a conventional ES (51). This is a complex installation of information security tools (MDZ, antivirus, etc.) on the computer and client OS in order to reduce the possibility of computer infection by malware (52).

Proposed model

Public key infrastructure provides integrity and verifies the authorship of each document. Timestamps certify the time a document was signed, which is essential for time-bound transactions, rejection, and data retention for audit. Of course, the entire document management system with digital signatures must comply with the requirements of the country of jurisdiction and the countries where partners and customers work. Uniform standards for electronic document management and digital signature infrastructure are gradually being developed. A class of applications provide a complete windowed user interface for performing client-side crypto operations. As a rule, some CIPF is used as a crypto-core. This is shown in **Figure 1**.

- Including file signature verification, chaining and revocation list verification, OCSP, and timestamp verification.
- File encryption including multiple responders.
- User certificate search and selection.
- Maintaining a database of responder certificates, integrating with a directory service (using LDAP protocol) to search for responder certificates.
- Key pair generation and certificate request generation.
- Import/export of certificates (root, user, and responders).

The providers of document management solutions or applications want to integrate digital signatures or stamps. Another option is to offer them as a premium option to customers as guaranteed document protection against fraud.

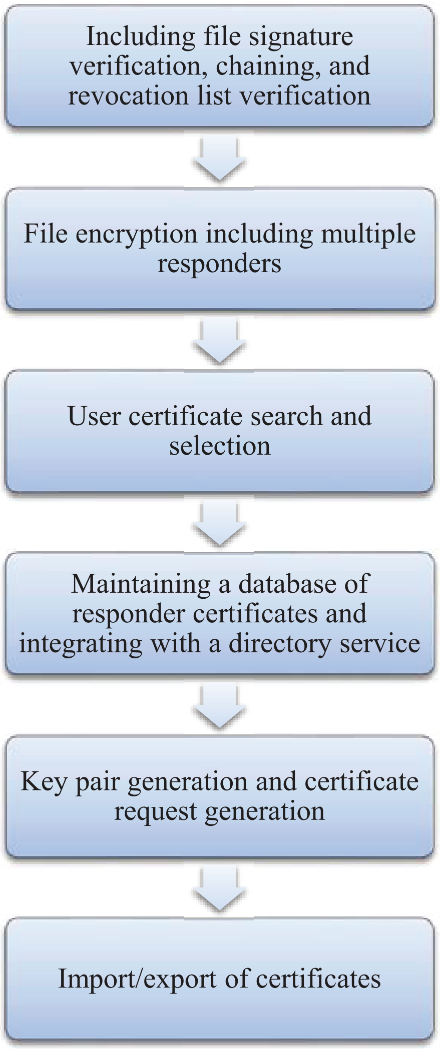
Including file signature verification, chaining, and revocation list verification
File encryption including multiple responders
User certificate search and selection
Maintaining a database of responder certificates and integrating with a directory service
Key pair generation and certificate request generation
Import/export of certificates

FIGURE 1 | User interface for performing client-side crypto operations.

A flexible model is supported here: digital signatures can be added as an additional or optional layer. Now, the businesses looking to integrate digital signatures or stamps are into their workflows. The system integrators are implementing the digital signatures in existing or new document management systems. The problem of creating a trusted environment for performing cryptooperations, especially EDS, is a separate big topic. This article does not plan to consider it in detail, but conceptually, developers go along the following lines.

- A separate device where the data for signature are displayed and the signature is performed after user confirmation (trust).
- Boot a separate trusted OS in USB-Live mode.
- Parallel operation of client OS and reliable environment on different cores of a computer.

All these documents are now sent in a long journey of communication between the accounting departments on the supplier's and the buyer's side. Although the problem of inconsistencies can be solved at the point of export, the fact of the change will be confirmed by a "Cloud" signature. This is shown in Figure 2.

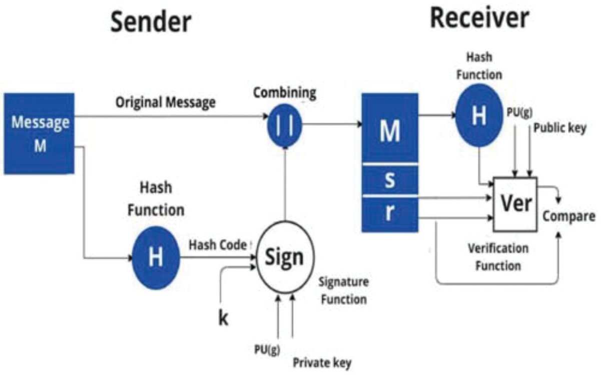

FIGURE 2 | Proposed model.

Currently, there are completely new developments using block chain technology, that is, smart contracts. "Distribution, the basic principle of the technology, provides complete protection against compromise and unauthorized access to any document or signature, because each such block element (signature, document, archive, etc.) is located in a strong chain of numbered blocks. Protected by a very complex cryptographic code. Making changes to a block already in circulation Not possible; a smart contract is an electronic mechanism that describes a set of conditions that will fulfill certain events." His work is based on the development and use of so-called low-trust protocols, where the protocol algorithm uses only software tools, and the human factor is excluded as much as possible from the decision-making chain – here A person acts exclusively.

Results and discussion

The proposed HKSS was compared with the existing e-diploma system model (EDSM), block chain-based Lamport Merkle digital signature (BLMDS), antivirus security systems (ASS), and structural digital signature (SDS).

Integration of applets

One of the options for using CIPF in the browser is their integration into Java applets. In some cases, CIPF and cryptographic libraries do not require installation and are native libraries. In this case, it can be integrated directly "inside" the applet and call CIPF functions through the Java Native Interface mechanism. With this scheme, when a Java applet is loaded in the browser for the first time, the library is installed in the user's profile, and its separate installation is not required. Another option is to write a Java applet that calls a pre-installed CIPF on the system (CSP, JCP, etc.). This is shown in **Figure 3**.

Development language management

PHP is one of the most widely used web development languages. The PHP cryptographic subsystem is built on Open SSL, which supports Russian cryptographic algorithms. At the same time, there is no support for Russian crypto algorithms in PHP. Some Russian CIPF manufacturers started to develop patches for PHP that would allow the use of Russian cryptography, but this work was not completed. This is shown in **Figure 4**.

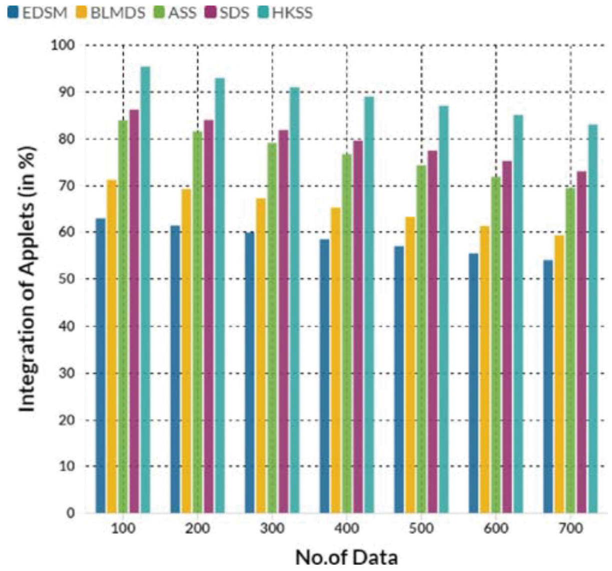

FIGURE 3 | Comparison of applets integration.

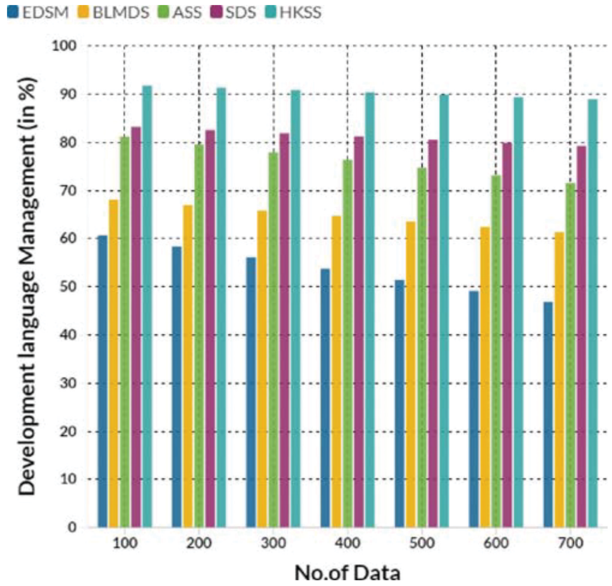

FIGURE 4 | Comparison of development language management.

Information systems management

Currently, many developers of PHP-based information systems use a direct call to the Open SSL command line utility to perform crypto operations. The attractive solution was implemented as part of the WEB project. In the server component of the solution, GOST R 34.10-2001 signature verification is implemented directly in PHP using mathematical primitives from the native library. This is shown in **Figure 5**.

In-house encryption management

Configuration and support require in-house encryption expertise. They go separately, require separate calls from

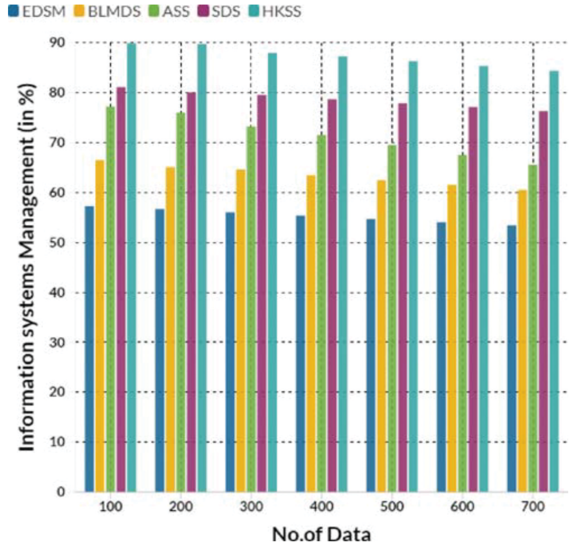

FIGURE 5 | Comparison of information systems management.

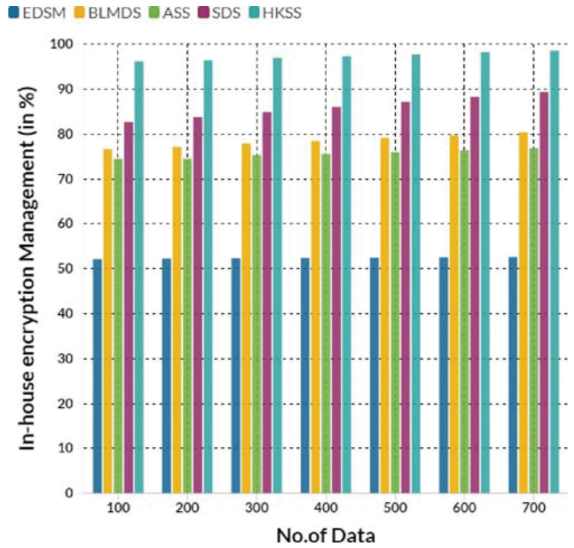

FIGURE 6 | Comparison of in-house encryption management.

built-in applications and internal development resources, and may require additional equipment purchase and configuration. This is shown in **Figure 6**.

Client responsibility for key management and storage is critical. Not all solutions support both types of identities. A cloud service greatly simplifies the deployment of a document management system with support for digital signatures. All operations go through the API. Binary compatibility of CIPF, such as Crypto Packet with Open SSL, makes it possible to provide legitimacy to this solution.

Conclusion

Cloud services vary in price and functionality. But they all guarantee flexibility, scalability, and high availability. Although the services are paid, companies are freed from the need to invest in the development of their own solutions, including the purchase of expensive cryptographic equipment. A cloud-based digital signature service may be required. In theory, these are companies of any size that develop or implement custom-built applications and want to integrate digital signatures or use an already integrated application. For example, when sending money, it is impossible to execute a contract without obtaining the number of ES specified in the contract. Talking about the spread of the practice of using "Cloud" ES and the possibilities of developing technologies, there is a problem. Today, it is connected with the fact that the problems of using such ES are not well spelled out in the regulations. So, companies will soon stop being afraid of "cloud" technologies and use such ES in their work even more. Expect to start using it in earnest.

References

1. Finandhita A, Afrianto I. Development of e-diploma system model with digital signature authentication. *Proceedings of the IOP Conference series: Materials science and engineering*. (Vol. 407), Bristol: IOP Publishing (2018). 12109 p.
2. Gopi B, Logeshwaran J, Kiruthiga T. An innovation in the development of a mobile radio model for a dual-band transceiver in wireless cellular communication. *BOHR Int J Comput Intell Commun Netw.* (2022) 1:20–5.
3. Alzubi JA. Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare. *Comput Commun.* (2021) 170:200–8.
4. Ramesh G, Logeshwaran J, Aravindarajan V. The performance evolution of antivirus security systems in ultra dense cloud server using intelligent deep learning. *BOHR Int J Comput Intell Commun Netw.* (2022) 1:15–9.
5. Lu CS, Liao HYM. Structural digital signature for image authentication: An incidental distortion resistant scheme. *Proceedings of the 2000 ACM workshops on multimedia*. New York, NY: Association for Computing Machinery (2000). p. 115–8.
6. Logeshwaran J. The control and communication management for ultra dense cloud system using fast Fourier algorithm. *ICTACT J Data Sci Mach Learn.* (2022) 3:281–4.
7. Warasart M, Kuacharoen P. Based document authentication using digital signature and QR code. *Proceedings of the 4th International conference on computer engineering and technology (ICCET 2012).* New York, NY: ASME Press (2012).
8. Gopi B, Ramesh G, Logeshwaran J. The fuzzy logical controller based energy storage and conservation model to achieve maximum energy efficiency in modern 5G communication. *ICTACT J Commun Technol.* (2022) 13:2774–9.
9. Dhagat R, Joshi P. New approach of user authentication using digital signature. *Proceedings of the 2016 Symposium on colossal data analysis and networking (CDAN)*. Piscataway, NJ: IEEE (2016). p. 1–3.
10. Ramesh G, Logeshwaran J, Gowri J, Mathew A. The management and reduction of digital noise in video image processing by using transmission based noise elimination scheme. *ICTACT J Image Video Process.* (2022) 13:2797–801.
11. Kazmirchuk S, Anna I, Sergii I. Digital signature authentication scheme with message recovery based on the use of elliptic curves. *Proceedings of the International conference on computer science, engineering and education applications*. Cham: Springer (2019). p. 279–88.
12. Gopi B, Ramesh G, Logeshwaran J. An innovation for energy release of nuclear fusion at short distance dielectrics in semiconductor model. *ICTACT J Microelectron.* (2022) 8:1430–5.
13. Lou DC, Liu JL. Fault resilient and compression tolerant digital signature for image authentication. *IEEE Trans Consum Electron.* (2000) 46:31–9.
14. Logeshwaran J, Rex MJ, Kiruthiga T, Rajan VA. FPSMM: Fuzzy probabilistic based semi morkov model among the sensor nodes for realtime applications. *Proceedings of the 2017 International conference on intelligent sustainable systems (ICISS)*. Piscataway, NJ: IEEE (2017). p. 442–6.
15. Chen T, Wang J, Zhou Y. Combined digital signature and digital watermark scheme for image authentication. *Proceedings of the 2001 International conferences on Info-Tech and Info-Net (Cat. No. 01EX479).* (Vol. 5), Piscataway, NJ: IEEE (2001). p. 78–82.
16. Ramesh G, Logeshwaran J, Rajkumar K. The smart construction for image preprocessing of mobile robotic systems using neuro fuzzy logical system approach. *Neuroquantology.* (2022) 20:6354–67.
17. Dittmann J, Steinmetz A, Steinmetz R. Content-based digital signature for motion pictures authentication and content-fragile watermarking. *Proceedings of the IEEE International conference on multimedia computing and systems*. (Vol. 2), Piscataway, NJ: IEEE (1999). p. 209–13.
18. Raja S, Logeshwaran J, Venkatasubramanian S, Jayalakshmi M, Rajeswari N, Olaiya NG, et al. OCHSA: designing energy-efficient lifetime-aware leisure degree adaptive routing protocol with optimal cluster head selection for 5G communication network disaster management. *Sci Program.* (2022) 2022:5424356.
19. Sagar Hossen M, Tabassum T, Islam A, Karim R, Rumi LS, Kobita AA. Digital signature authentication using asymmetric key cryptography with different byte number. *Proceedings of the ICECMSN 2020, evolutionary computing and mobile sustainable networks*. Singapore: Springer (2021). p. 845–51.
20. Logeshwaran J, Shanmugasundaram RN. Enhancements of resource management for device to device (D2D) communication: A review. *Proceedings of the 2019 Third international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. Piscataway, NJ: IEEE (2019). p. 51–5.
21. Karim R, Rumi LS, Islam A, Kobita AA, Tabassum T, Sagar Hossen M. Digital signature authentication for a bank using asymmetric key cryptography algorithm and token based encryption. *Proceedings of the ICECMSN 2020, evolutionary computing and mobile sustainable networks*. Singapore: Springer (2021). p. 853–9.
22. Gopi B, Logeshwaran J, Gowri J, Kiruthiga T. The moment probability and impacts monitoring for electron cloud behavior of electronic computers by using quantum deep learning model. *Neuroquantology.* (2022) 20:6088–100.
23. Alam S, Jamil A, Saldhi A, Ahmad M. Digital image authentication and encryption using digital signature. *Proceedings of the 2015 International*

conference on advances in computer engineering and applications. Piscataway, NJ: IEEE (2015). p. 332–6.

24. Logeshwaran J. AICSA - an artificial intelligence cyber security algorithm for cooperative P2P file sharing in social networks. *ICTACT J Data Sci Mach Learn.* (2021) 3:251–3.
25. Alizai ZA, Tareen NF, Jadoon I. Improved IoT device authentication scheme using device capability and digital signatures. *Proceedings of the 2018 International conference on applied and engineering mathematics (ICAEM)*. Piscataway, NJ: IEEE (2018). p. 1–5.
26. Gopi B, Logeshwaran J, Gowri J, Aravindarajan V. The identification of quantum effects in electronic devices based on charge transfer magnetic field model. *Neuroquantology.* (2022) 20:5999–6010.
27. Choudhury N, Matam R, Mukherjee M, Lloret J. A performance-to-cost analysis of IEEE 802.15. 4 MAC with 802.15. 4e MAC modes. *IEEE Access.* (2020) 8:41936–50.
28. Logeshwaran J, Adhikari N, Joshi SS, Saxena P, Sharma A. The deep DNA machine learning model to classify the tumor genome of patients with tumor sequencing. *Int J Health Sci.* (2022) 6:9364–75.
29. Moravejosharieh A, Lloret J. Performance evaluation of co-located IEEE 802.15. 4-based wireless body sensor networks. *Ann Telecommun.* (2016) 71:425–40.
30. Logeshwaran J, Malik JA, Adhikari N, Joshi SS, Bishnoi P. IoT-TPMS: an innovation development of triangular patient monitoring system using medical internet of things. *Int J Health Sci.* (2022) 6:9070–84.
31. Choudhury N, Matam R, Mukherjee M, Lloret J. LBS: a beacon synchronization scheme with higher schedulability for IEEE 802.15. 4 cluster-tree-based IoT applications. *IEEE Internet Things J.* (2019) 6:8883–96.
32. Ramesh G, Aravindarajan V, Logeshwaran J, Kiruthiga T, Vignesh S. Estimation analysis of paralysis effects for human nervous system by using neuro fuzzy logic controller. *Neuroquantology.* (2022) 20: 3195–206.
33. Choudhury N, Matam R, Mukherjee M, Lloret J, Kalaimannan E. NCHR: a nonthreshold-based cluster-head rotation scheme for IEEE 802.15. 4 cluster-tree networks. *IEEE Internet Things J.* (2020) 8: 168–78.
34. Ramesh G, Logeshwaran J, Aravindarajan V, Thachil F. Eliminate the interference in 5G ultra-wide band communication antennas in cloud computing networks. *ICTACT J Microelectron.* (2022) 8: 1338–44.
35. Yassin AA, Jin H, Ibrahim A, Zou D. Anonymous password authentication scheme by using digital signature and fingerprint in cloud computing. *Proceedings of the 2012 Second International conference on cloud and green computing*. Piscataway, NJ: IEEE (2012). p. 282–9.
36. Sekar G, Sivakumar C, Logeshwaran J. NMLA: the smart detection of motor neuron disease and analyze the health impacts with neuro machine learning model. *Neuroquantology.* (2022) 20:892–9.
37. Ferng HW, Khoa NM. On security of wireless sensor networks: a data authentication protocol using digital signature. *Wirel Netw.* (2017) 23:1113–31.
38. Logeshwaran J, Karthick S. A smart design of a multi-dimensional antenna to enhance the maximum signal clutch to the allowable standards in 5G communication networks. *ICTACT J Microelectron.* (2022) 8:1269–74.
39. Anderson R, Bergadano F, Crispo B, Lee JH, Manifavas C, Needham R. A new family of authentication protocols. *ACM SIGOPS Oper Syst Rev.* (1998) 32:9–20.
40. Jasmine J, Yuvaraj N, Logeshwaran J editors. DSQLR-A distributed scheduling and QoS localized routing scheme for wireless sensor network. *Recent trends in information technology and communication for industry 4.0*, Chennai: RcHuB Publications (2022). p. 47–60.
41. Raja S, Rajan AJ. A decision-making model for selection of the suitable FDM machine using fuzzy TOPSIS. *Math Probl Eng.* (2022) 2022:15.
42. Ramkumar M, Logeshwaran J, Husna T. CEA: certification based encryption algorithm for enhanced data protection in social networks. *Fundam Appl Math Soft Comput.* (2022) 1:161–70.
43. Venkatasubramanian S, Raja S, Sumanth V, Dwivedi JN, Sathiaparkavi J, Modak S, et al. Fault diagnosis using data fusion with ensemble deep learning technique in IIoT. *Math Probl Eng.* (2022) 2022:1–8.
44. Logeshwaran J, Ramkumar M, Kiruthiga T, Sharan Pravin R. SVPA - the segmentation based visual processing algorithm (SVPA) for illustration enhancements in digital video processing (DVP). *ICTACT J Image Video Process.* (2022) 12:2669–73.
45. Mehbodniya A, Webber JL, Neware R, Arslan F, Pamba RV, Shabaz M. Modified Lamport Merkle digital signature blockchain framework for authentication of internet of things healthcare data. *Expert Syst.* (2022) 39:e12978.
46. Logeshwaran J, Ramkumar M, Kiruthiga T, Sharanpravin R. The role of integrated structured cabling system (ISCS) for reliable bandwidth optimization in high-speed communication network. *ICTACT J Commun Technol.* (2022) 13:2635–9.
47. Singh M, Kaur H, Kakkar A. Digital signature verification scheme for image authentication. *Proceedings of the 2015 2nd International conference on recent advances in engineering & computational sciences (RAECS)*. Piscataway, NJ: IEEE (2015). p. 1–5.
48. Logeshwaran J, Saravanakumar K, Dineshkumar S, Arunprasath C. SBML algorithm for intelligent fuel filling (IFF) and smart vehicle identification system (SVIS). *Int J Adv Res Manag Archit Technol Eng.* (2016) 2:149–54.
49. Murty MS, Veeraiah D, Rao AS. Digital signature and watermark methods for image authentication using cryptography analysis. *Signal Image Process.* (2011) 2:170–9.
50. Saravanakumar K, Logeshwaran J. Auto-Theft prevention system for underwater sensor using lab view. *Int J Innov Res Comput Commun Eng.* (2016) 4:1750–5.
51. Ganeshkumar K, Arivazhagan D. Generating a digital signature based on new cryptographic scheme for user authentication and security. *Indian J Sci Technol.* (2014) 7:1–5.
52. Sutharasan M, Logeshwaran J. Design intelligence data gathering and incident response model for data security using honey pot system. *Int J Res Dev Technol.* (2016) 5:310–4.