Shashank Gupta

List of Publications by Year
in descending order

46 papers	1,001 citations	471371 17 h-index	454834 30 g-index
48 all docs	48 docs citations	48 times ranked	453 citing authors

#	Article	IF	Citations
1	Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: a survey, current challenges and future directions. Journal of Ambient Intelligence and Humanized Computing, 2023, 14, 361-407.	3.3	63
2	A way forward towards a technology‐driven development of industry 4.0 using big data analytics in 5G‐enabled IIoT. International Journal of Communication Systems, 2022, 35, .	1.6	11
3	Achieving Ambient Intelligence in Addressing the COVID-19 Pandemic Using Fog Computing-Driven IoT. Advances in Systems Analysis, Software Engineering, and High Performance Computing Book Series, 2022, , 56-92.	0.5	1
4	Fog computing in enabling 5G-driven emerging technologies for development of sustainable smart city infrastructures. Cluster Computing, 2022, 25, 1111-1154.	3.5	17
5	ConvXSS: A deep learning-based smart ICT framework against code injection attacks for HTML5 web applications in sustainable smart city infrastructure. Sustainable Cities and Society, 2022, 80, 103765.	5.1	10
6	An Upgraded Object Detection Model for Enhanced Perception and Decision Making in Autonomous Vehicles. , 2022, , .		1
7	Framework for determining the suitability of blockchain: Criteria and issues to consider. Transactions on Emerging Telecommunications Technologies, 2021, 32, e4334.	2.6	11
8	A survey on the role of Internet of Things for adopting and promoting Agriculture 4.0. Journal of Network and Computer Applications, 2021, 187, 103107.	5.8	92
9	Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. Ad Hoc Networks, 2021, 123, 102685.	3.4	54
10	Detecting Different Attack Instances of DDoS Vulnerabilities on Edge Network of Fog Computing using Gaussian Naive Bayesian Classifier. , 2020, , .		7
11	Designing a XSS Defensive Framework for Web Servers Deployed in the Existing Smart City Infrastructure. Journal of Organizational and End User Computing, 2020, 32, 85-111.	1.6	18
12	Future IoT‐enabled threats and vulnerabilities: State of the art, challenges, and future prospects. International Journal of Communication Systems, 2020, 33, e4443.	1.6	18
13	A client‐server JavaScript code rewriting‐based framework to detect the XSS worms from online social network. Concurrency Computation Practice and Experience, 2019, 31, e4646.	1.4	6
14	A Framework for Preserving the Privacy of Online Users Against XSS Worms on Online Social Network. International Journal of Information Technology and Web Engineering, 2019, 14, 85-111.	1.2	5
15	SEC‐H5: Secure and efficient integration of settings of enhanced HTML5 XSS vector defensive framework on edge network of fog nodes. Concurrency Computation Practice and Experience, 2019, 31, e5188.	1.4	2
16	Evaluation and monitoring of XSS defensive solutions: a survey, open research issues and future directions. Journal of Ambient Intelligence and Humanized Computing, 2019, 10, 4377-4405.	3.3	3
17	Development of IoT for Smart Agriculture a Review. Advances in Intelligent Systems and Computing, 2019, , 425-432.	0.5	48
18	Efficient yet Robust Elimination of XSS Attack Vectors from HTML5 Web Applications Hosted on OSN-Based Cloud Platforms. Procedia Computer Science, 2018, 125, 669-675.	1.2	10

#	ARTICLE	IF	CITATIONS
19	XSS-secure as a service for the platforms of online social network-based multimedia web applications in cloud. Multimedia Tools and Applications, 2018, 77, 4829-4861.	2.6	56
20	Hunting for DOM-Based XSS vulnerabilities in mobile cloud-based online social network. Future Generation Computer Systems, 2018, 79, 319-336.	4.9	37
21	POND: polishing the execution of nested context-familiar runtime dynamic parsing and sanitisation of XSS worms on online edge servers of fog computing. International Journal of Innovative Computing and Applications, 2018, 9, 116.	0.2	3
22	Robust injection point-based framework for modern applications against XSS vulnerabilities in online social networks. International Journal of Information and Computer Security, 2018, 10, 170.	0.2	5
23	SFC: A Three Layer Smart Phone-Fag-Cloud Framework for Defending Against JavaScript Code Injection Vulnerabilities on OSN. , 2018, , .		2
24	Defense Against HTML5 XSS Attack Vectors: A Nested Context-Aware Sanitization Technique. , 2018, , .		4
25	DOM-Guard: Defeating DOM-Based Injection of XSS Worms in HTML5 Web Applications on Mobile-Based Cloud Platforms. , 2018, , 425-454.		3
26	RAJIVE: restricting the abuse of JavaScript injection vulnerabilities on cloud data centre by sensing the violation in expected workflow of web applications. International Journal of Innovative Computing and Applications, 2018, 9, 13.	0.2	2
27	Enhancing the Browser-Side Context-Aware Sanitization of Suspicious HTML5 Code for Halting the DOM-Based XSS Vulnerabilities in Cloud. , 2018, , 216-247.		0
28	Robust injection point-based framework for modern applications against XSS vulnerabilities in online social networks. International Journal of Information and Computer Security, 2018, 10, 170.	0.2	3
29	Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. International Journal of Systems Assurance Engineering and Management, 2017, 8, 512-530.	1.5	117
30	Detection, Avoidance, and Attack Pattern Mechanisms in Modern Web Application Vulnerabilities. International Journal of Cloud Applications and Computing, 2017, 7, 1-43.	1.1	46
31	Smart XSS Attack Surveillance System for OSN in Virtualized Intelligence Network of Nodes of Fog Computing. International Journal of Web Services Research, 2017, 14, 1-32.	0.5	18
32	Enhancing the Browser-Side Context-Aware Sanitization of Suspicious HTML5 Code for Halting the DOM-Based XSS Vulnerabilities in Cloud. International Journal of Cloud Applications and Computing, 2017, 7, 1-31.	1.1	39
33	JSâ€SAN: defense mechanism for HTML5â€based web applications against javascript code injection vulnerabilities. Security and Communication Networks, 2016, 9, 1477-1495.	1.0	28
34	Automated Discovery of JavaScript Code Injection Attacks in PHP Web Applications. Procedia Computer Science, 2016, 78, 82-87.	1.2	17
35	XSSâ€immune: a Google chrome extensionâ€based XSS defensive framework for contemporary platforms of web applications. Security and Communication Networks, 2016, 9, 3966-3986.	1.0	15
36	Enhanced XSS Defensive Framework for Web Applications Deployed in the Virtual Machines of Cloud Computing Environment. Procedia Technology, 2016, 24, 1595-1602.	1.1	20

#	Article	IF	Citations
37	CSSXC: Context-sensitive Sanitization Framework for Web Applications against XSS Vulnerabilities in Cloud Environments. Procedia Computer Science, 2016, 85, 198-205.	1.2	18
38	An Infrastructure-Based Framework for the Alleviation of JavaScript Worms from OSN in Mobile Cloud Platforms. Lecture Notes in Computer Science, 2016, , 98-109.	1.0	13
39	Alleviating the proliferation of JavaScript worms from online social network in cloud platforms. , 2016, , .		8
40	XSS-SAFE: A Server-Side Approach to Detect and Mitigate Cross-Site Scripting (XSS) Attacks in JavaScript Code. Arabian Journal for Science and Engineering, 2016, 41, 897-920.	1.1	44
41	Auditing Defense against XSS Worms in Online Social Network-Based Web Applications. Advances in Information Security, Privacy, and Ethics Book Series, 2016, , 216-245.	0.4	18
42	Efficient Service Utilization in Cloud Computing Exploitation Victimization as Revised Rough Set Optimization Service Parameters. Procedia Computer Science, 2015, 70, 610-617.	1.2	19
43	PHP-sensor. , 2015, , .		43
44	BDS. Advances in Information Security, Privacy, and Ethics Book Series, 2015, , 174-191.	0.4	21
45	Exploitation of Cross-Site Scripting (XSS) Vulnerability on Real World Web Applications and its Defense. International Journal of Computer Applications, 2012, 60, 28-33.	0.2	18
46	Smart XSS Attack Surveillance System for OSN in Virtualized Intelligence Network of Nodes of Fog Computing. , 0, , 332-364.		0