Scalable and secure bigdata IoT system based on multi factor authentication and lightweight cryptography

Author-1: Mr. M. Santhosh kumar
Assistant Professor, Department of Computer science Engineering, Geethanjali college of Engineering and Technology, Hyderabad, Telangana, India.
Author-2: Mr. C. Vikas
Assistant Professor, Department of Computer science Engineering, Geethanjali college of Engineering and Technology, Hyderabad, Telangana, India.
Author-3: Mrs. P. Archana
Assistant Professor, Department of Computer science Engineering, Geethanjali college of Engineering and Technology, Hyderabad, Telangana, India.

.

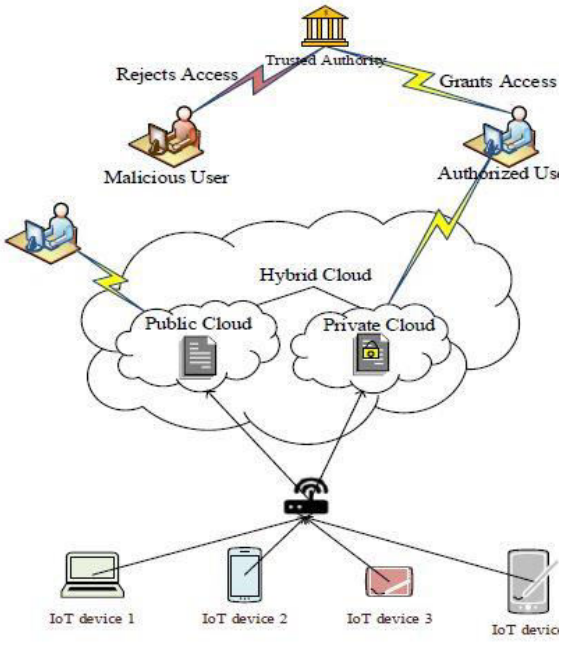
Abstract:-

Organizations share an evolving interest in adopting a cloud computing approach for Internet of Things (IoT) applications. Integrating IoT devices and cloud computing technology is considered as an effective approach to storing and managing the enormous amount of data generated by various devices. However, big data security of these organizations presents a challenge in the IoT–cloud architecture. To overcome security issues, we propose a cloud-enabled IoT environment supported by multifactor authentication and lightweight cryptography encryption schemes to protect big data system. The proposed hybrid cloud environment is aimed at protecting organizations' data in a highly secure manner. The hybrid cloud environment is a combination of private and public cloud. Our IoT devices are divided into sensitive and nonsensitive devices. Sensitive devices generate sensitive data, such as healthcare data; whereas nonsensitive devices generate nonsensitive data, such as home appliance data. IoT devices send their data to the cloud via a gateway device. Herein, sensitive data are split into two parts: one part of the data is encrypted using RC6, and the other part is encrypted using the Fiestel encryption scheme. Nonsensitive data are encrypted using the Advanced Encryption Standard (AES) encryption scheme. Sensitive and nonsensitive data are respectively stored in private and public cloud to ensure high security. The use of multifactor authentication to access the data stored in the cloud is also proposed. During login, data users send their registered credentials to the Trusted Authority (TA). The TA provides three levels of authentication to access the stored data: first-level authentication - read file, second-level authentication - download file, and third-level authentication - download file from the hybrid cloud. We implement the proposed cloud–IoT architecture in the NS3 network simulator. We evaluated the performance of the proposed architecture using metrics such as computational time, security strength, encryption time, and decryption time.

Keywords— cloud computing, Internet of Things, lightweight cryptography encryption, big data.

INTRODUCTION

In accordance with the advancement and wide use of Internet of Things (IoT) applications and with the emergence of wireless communication and mobile technologies, IoT and cloud computing have become important concepts. IoT aims to provide connectivity for anything with minimum storage and computing capabilities [1] [2]. Security is a major issue in cloud-integrated IoT, and the user data stored in the cloud requires secure protection
[3]. A lightweight multifactor secured smart card-based user authentication is introduced in cloud–IoT applications [4]. Figure 1 shows the architecture for cloud-integrated IoT, which consists of the hybrid cloud, IoT devices, and users. The hybrid cloud includes public and private cloud. The public cloud is used to store nonsensitive data, whereas the private cloud is used to store highly sensitive data.



require to supply their biometrics, alongside factor finger print as well as moreover retina, to the TA. After that, the TA validates the supplied certifications rather than signed up qualifications. If the verification is a fulfillment, after that the TA gives The stop-to-stop safe and relaxed interplay format is suggested for a cloud-associated Iota environment. Below, a minimum software program software protocol is usually urged for a relaxed discussion between Iota as well as likewise the cloud [5] A homomorphism safety device primarily based totally on the hoop reading extra about with mistakes components is applied for cloud consumer verification [6] Role-primarily based accessibility address (RBAC) with the rely on assessment (TE) collection of plans is carried out to use get proper of accessibility to control to Iota properties. RBAC consists of three TE formulation,
particularly, community presume assessment formulation, digital rely on evaluation set of rules, in addition to cooperative take delivery of as true with evaluation collection of hints [7] A moderate-weight Iota-based totally absolutely cryptography verification method is provided to supply safety in a cloud-- Iota environments. An advised light-weight affirmation plan embraces a one-way hash precise in addition to positive OR method [8] a modern light-weight verification plan based clearly upon expert alongside aspect big informal safety and protection evaluation is suggested for a cloud-assisted Iota environments. Official protection examination is completed via a random oracle fashion [9] an approve as actual with-based Iota cloud putting is delivered to offer a hazard-free similarly to comfy storage in a cloud surroundings. The beyond realities of every Iota system is amassed making use of a centralized Iota take delivery of as authentic with method assumption more or less for safety exam [10] A cozy and additionally in addition licensed ordinary assessment structure (SCCAF) is recommended to cozy purchaser realities in a cloud-assisted Iota setting. The SCCAF substances guidelines for cloud people in evaluating the protection and additionally

protection along with consistency fees of cloud organization [11] Lightweight context-conscious Iota solutions are supplied to the individual. In addition, the surpassed light-weight context-conscious solution makes use of a clean out to beforehand some of the maximum appropriate information to customers at the principle in their context [12] The blurry logical ordered system (FAHP) additives is recommended to analyze the famous consider Iota. The FAHP gives an amazing evaluation of specific variables, particularly, safety, rate, in addition to connection [13] a moderate-weight bootstrapping gadget is used for secure Iota solutions. The Ephemeral Daffier-- Hellman over COSE method is implemented to standardize vital agreements in Iota gizmos [14]

The vital feature of the dominating art work is to signify a multilevel affirmation scheme that can provide advanced protection in integrated Iota-- cloud surroundings. The essential fees of these paints are summarized as observe:

➢ It suggests a hybrid cloud which consist of brilliant in addition to public cloud that might improve the safety of Iota systems. Iota gear is moreover dividing right into sensitive along with no sensitive gadgets on the idea of the shape of truths generated.

➢ the safety of touchy facts from sensitive gadgets is assured with the beneficial deliver of securing them making use of RC6 in addition to in addition the Fiesta safety machine. The encrypted sensitive information are stored in a high-quality cloud the usage of an entryway device to supply excessive defense and moreover safety.

➢ No sensitive records from no sensitive gadgets are encrypted via the AES approach and afterward stored in a public cloud thru a front tool.

➢ to relaxed cloud-stored files from negative customers, this ardor advises a multilevel authentication device with counted on authority (TA). The multilevel confirmation device is partitioned into three arrays, even though that consists of (TA) to the recommended Cloud-Iota Atmosphere will surely intention more cloud solution price, taken into consideration that the Atmosphere will honestly clear up 1/3 birthday celebration answer.

➢ to stop dangerous humans from assessing saved info, this hobby recommends a number one-degree authentication maker. At this diploma, humans need to supply their person ID and also password to the TA. Afterwards, the TA verifies the ones certifications in competition to joined qualifications. If the verification attains success, after that the TA provides the customers reap admission to observe the files; otherwise, it rejects the ask for solve of access to.

➢ To hold you unapproved people from downloading and installation facts, this charge of hobby offers a second-diploma verification scheme wherein individuals the people availability to down fill papers; in another example, it denies the ask for advantage obtain admission to.

➢ the very last degree of confirmation is generally sponsored to cozy the data from

unauthorized assessment on the side of downloading. At this stage, customers need to offer their man or woman ID, password, and additionally furthermore biometrics to the TA. Then, the TA confirms the supplied qualifications in vicinity of subscribed credentials. If the confirmation is a success, afterwards the TA makes use of the clients ease of get entry to down fill and moreover installation similarly to test the statistics from the cloud; otherwise, it refutes the request for advantage get right of the front to.

LITERARY WORKS SURVEY

1. A Lightweight Client Authentication Plan for Cloud-Iota Based Doctor With the persistent transformation of cloud computing as well as Internet of Details, a few range flung patron tracking has ended up being feasible. These networking requirements are particularly associated with offer medical care solutions and real-time character surveillance. The picking up gizmos which can be each wearable or embedded inside the body of a male or woman delivers purchaser's records to the away scientific facilities. The well-being professional can get right of entry to character's realities saved within the cloud almost anywhere round the sector. As the touchy realities of the persona are dispatched over troubled cloud-Iota networks, comfy individual authentication is of extreme fee. A green private verification machine makes certain that actually genuine human beings can get right of get admission to statistics in addition to options. This paper recommends a protected and also at ease and also powerful purchaser authentication scheme for far off man or woman monitoring. The supported plan is prolonged long-term, lightweight and comfy and defend in place of some of safety and safety assaults. In addition, the tool has low computational overhead. A genuine confirmation using AVISPA device confirms the protection and safety and protection of the advocated device.

2. A useful and additionally energy-inexperienced taking component haze company for Iota answers. Fog-to-fog verbal exchange has been introduced to deliver offerings to clients with very little dependence on the cloud through deliver and also functionality sharing of taking factor hazes. Existing offerings prepare for entire partnership some of the hazes to provide clean more too composite offerings. Fairly, each haze can furthermore further originated from a completely splendid community driving force or issuer company and further due to this will without a doubt no longer take part in any shape of type of partnership up until self-economic income is maintained. In this paper, we offer a haze collaboration method for clean in addition to complicated multimedia address freight to tail clients even as impediment common income for the deciding on strolls with every other fog. The stop-to-stop safe and relaxed interplay format is suggested for a cloud-associated Iota environment. Below, a minimum software program software protocol is usually urged for a relaxed discussion between Iota as well as likewise the cloud [5] A homomorphism safety device primarily based totally on the hoop reading extra about with mistakes components is applied for cloud consumer verification [6] Role-primarily based accessibility address (RBAC) with the rely on assessment (TE) collection of plans is carried out to use get proper of

accessibility to control to Iota properties. RBAC consists of three TE formulation, particularly, community presume assessment formulation, digital rely on evaluation set of rules, in addition to cooperative take delivery of as true with evaluation collection of hints [7] A moderate-weight Iota-based totally absolutely cryptography verification method is provided to supply safety in a cloud-- Iota environments. An advised light-weight affirmation plan embraces a one-way hash precise in addition to positive OR method [8] a modern light-weight verification plan based clearly upon expert alongside aspect big informal safety and protection evaluation is suggested for a cloud-assisted Iota environments. Official protection examination is completed via a random oracle fashion [9] an approve as actual with-based Iota cloud putting is delivered to offer a hazard-free similarly to comfy storage in a cloud surroundings. The beyond realities of every Iota system is amassed making use of a centralized Iota take delivery of as authentic with method assumption more or less for safety exam [10] A cozy and additionally in addition licensed ordinary assessment structure (SCCAF) is recommended to cozy purchaser realities in a cloud-assisted Iota setting. The SCCAF substances guidelines for cloud people in evaluating the protection and additionally protection along with consistency fees of cloud organization [11] Lightweight context-conscious Iota solutions are supplied to the individual. In addition, the surpassed light-weight context-conscious solution makes use of a clean out to beforehand some of the maximum appropriate information to customers at the principle in their context [12] The blurry logical ordered system (FAHP) additives is recommended to analyze the famous consider Iota. The FAHP gives an amazing evaluation of specific variables, particularly, safety, rate, in addition to connection [13] a moderate-weight bootstrapping gadget is used for secure Iota solutions. The Ephemeral Daffier-- Hellman over COSE method is implemented to standardize vital agreements in Iota gizmos [14]

The vital feature of the dominating art work is to signify a multilevel affirmation scheme that can provide advanced protection in integrated Iota-- cloud surroundings. The essential fees of these paints are summarized as observe:

➢ It suggests a hybrid cloud which consist of brilliant in addition to public cloud that might improve the safety of Iota systems. Iota gear is moreover dividing right into sensitive along with no sensitive gadgets on the idea of the shape of truths generated.

➢ the safety of touchy facts from sensitive gadgets is assured with the beneficial deliver of securing them making use of RC6 in addition to in addition the Fiesta safety machine. The encrypted sensitive information are stored in a high-quality cloud the usage of an entryway device to supply excessive defense and moreover safety.

➢ No sensitive records from no sensitive gadgets are encrypted via the AES approach and afterward stored in a public cloud thru a front tool.

➢ to relaxed cloud-stored files from negative customers, this ardor advises a multilevel authentication device with counted on authority

(TA). The multilevel confirmation device is partitioned into three arrays, even though that consists of (TA) to the recommended Cloud-Iota Atmosphere will surely intention more cloud solution price, taken into consideration that the Atmosphere will honestly clear up 1/3 birthday celebration answer.

➢ to stop dangerous humans from assessing saved info, this hobby recommends a number one-degree authentication maker. At this diploma, humans need to supply their person ID and also password to the TA. Afterwards, the TA verifies the ones certifications in competition to joined qualifications. If the verification attains success, after that the TA provides the customers reap admission to observe the files; otherwise, it rejects the ask for solve of access to.

➢ To hold you unapproved people from downloading and installation facts, this charge of hobby offers a second-diploma verification scheme wherein individuals require to supply their biometrics, alongside factor finger print as well as moreover retina, to the TA. After that, the TA validates the supplied certifications rather than signed up qualifications. If the verification is a fulfillment, after that the TA gives the people availability to down fill papers; in another example, it denies the ask for advantage obtain admission to.

➢ the very last degree of confirmation is generally sponsored to cozy the data from unauthorized assessment on the side of downloading. At this stage, customers need to offer their man or woman ID, password, and additionally furthermore biometrics to the TA. Then, the TA confirms the supplied qualifications in vicinity of subscribed credentials. If the confirmation is a success, afterwards the TA makes use of the clients ease of get entry to down fill and moreover installation similarly to test the statistics from the cloud; otherwise, it refutes the request for advantage get right of the front to.

2.1 With the persistent transformation of cloud computing as well as Internet of Details, a few range flung patron tracking has ended up being feasible. These networking requirements are particularly associated with offer medical care solutions and real-time character surveillance. The picking up gizmos which can be each wearable or embedded inside the body of a male or woman delivers purchaser's records to the away scientific facilities. The well-being professional can get right of entry to character's realities saved within the cloud almost anywhere round the sector. As the touchy realities of the persona are dispatched over troubled cloud-Iota networks, comfy individual authentication is of extreme fee. A green private verification machine makes certain that actually genuine human beings can get right of get admission to statistics in addition to options. This paper recommends a protected and also at ease and also powerful purchaser authentication scheme for far off man or woman monitoring. The supported plan is prolonged long-term, lightweight and comfy and defend in place of some of safety and safety assaults. In addition, the tool has low computational overhead. A genuine confirmation using AVISPA device confirms the protection and safety and protection of the advocated device.

2.2 A useful and additionally energy-inexperienced taking component haze company for Iota answers. Fog-to-fog verbal exchange has been introduced to deliver offerings to clients with very little dependence on the cloud through deliver and also functionality sharing of taking factor hazes. Existing offerings prepare for entire partnership some of the hazes to provide clean more too composite offerings. Fairly, each haze can furthermore further originated from a completely splendid community driving force or issuer company and further due to this will without a doubt no longer take part in any shape of type of partnership up until self-economic income is maintained. In this paper, we offer a haze collaboration method for clean in addition to complicated multimedia address freight to tail clients even as impediment common income for the deciding on strolls with every other fog. The advised amusement activity dynamically produces quick-time period carrier-level setups (SLAs) supplied to shadow clients for company shipping at the identical time as taking complete benefit of guy or woman take delight in enhancement to haze earnings. The desire components and know-how mechanism that is based absolutely upon online in addition to offline simulation consequences to create confident technique for extremely-modern-day carrier company demands. The configuration specifications of the short SLAs are acquired the use of a modified taboo-based totally genuinely are looking for tool that uses preceding offerings at the same time as choosing logo-new maximum remarkable beneficial options. Efficiency evaluation influences reveal big income when it comes to provider delivery achievement price, company pinnacle notable, reduced durability consumption for haze even more to cloud datacenters, and moreover boosted fog income.

3. Shield Mix of Iota further to Cloud Computer Fog-to-fog communication has been given deliver answers to clients with low dependence on the cloud via precious aid alongside standard performance sharing of taking part fogs. Current services anticipate entire teamwork masses of the hazes to supply honest and moreover composite answers. Realistically, each haze can likewise originate from a diverse neighborhood element pressure or enterprise and therefore will genuinely not belong of any form of form of partnership till self-economic sales are continued. In this paper, we present a haze collaboration method for sincere similarly to further complex multimedia respond to shipping to tail customers whilst challenge shared income profits for the complying hazes. The recommended manner dynamically produces short-term issuer-diploma contracts (SLAs) given to shadow subscribers for answer freight on the same time as taking complete gain of purchaser pleasure additionally to haze income gains. The provider offers a getting know-how of gadget that trusts on line and also additionally offline simulation results to installation sure procedure for brand-new alternative requests. The setup requirements of the short-lived SLAs are gotten the use of a changed taboo-primarily based are trying to find tool that makes use of coming in advance than alternatives at the same time as choosing brand-new easy alternatives. Performance exam results display huge gains whilst it come to answer cargo accomplishment charge, provider agency splendid, lessened power usage for haze further to moreover cloud datacenters, in addition to furthermore multiplied fog profits.

4. A Light-weight Multi-Factor Secure Smart Card Based Remote Person Authentication System for Cloud-Iota Applications

With the fast get to the lowest of cloud laptop at the facet of ever earlier than raising large facts generated by using manner of Internet of Points (Iota), some distance character confirmation places the ultimate preliminary rate problem. Internet of Things is a paradigm wherein every tool within the Web Facilities (II) is adjoined right into a globally dynamic widening place. This paper suggests a distinct some distance off purchaser authentication plan for cloud-Iota packages. The gadget is moderate-weight in addition to sturdy to motions along aspect likewise has reduced computational overhead. The endorsed device pleases the popular essential traits of safety and protection. A formal verification did the use of AVISPA tool verifies the safety of the proposed technique

5. Secure Sense: End-to-End Secure Communication Style for the Cloud-Connected Net of Points Constricted Application Treatment (Coop) has undeniably emerged as the de-facto net demand for the Iota. Unlike stylish wireless sensing unit networks, Internet-associated exquisite factor executions require protection. Coop mandates the use of the Datagram TLS (DTLS) method because of the truth that the underlying included communication method. In this paper we perform DTLS-included relaxed in addition to unwanted Coop for each useful beneficial resource-restrained Iota devices in addition to also a cloud backend similarly to check all 3 security modes (pre-shared thriller, uncooked-public key, similarly to likewise certificate-primarily based virtually really) of Coop in a actual cloud-related Iota setup. We amplify SicsthSense-- a cloud gadget for the Iota-- with included Coop skills, in addition to reward a DTLS execution for treasured aid-limited Iota gadgets with raw-public mystery furthermore to certificates-based definitely jagged cryptography. To the very satisfactory of our competence, that is the preliminary attempt in the course of giving surrender-to-prevent danger-loose speak among useful resource-restrained smart elements further to cloud as soon as greater-ends which sustains all 3 protection setups of Coop each at the client aspect and moreover the net server trouble. Secure Sense-- our End-to-End (E2E) secure and relaxed conversation layout for the Iota-- includes all stylish-primarily based procedures, and moreover execution of these strategies are open provide as well as BSD-licensed. The Secure Sense evaluation standards and additionally furthermore open beneficial resource further to open up allow software program make it possible for future Iota product and offerings groups to make up safety and protection overhead whilst making use of all standardized strategies and additionally as making sure interoperability amongst numerous distributors. The center contributions of this paper are: (I) a whole implementation for Coop defense settings for E2E Iota protection, (ii) Iota safety likewise to verbal exchange techniques for a cloud platform for the Iota, in addition to (iii) entire experimental evaluation further to moreover benchmarking of E2E protection in amongst a community of smart factors and a cloud platform.

6. A Style of Secure Communication Procedure Making Use of RLWE-Based Homomorphism Security in Iota Merging Cloud Setup An

especially suitable-linked way of life is occurring in which issues and additionally subjects or people and moreover in addition directs connect with every diverse via the Internet of Points. Given that gadgets inner in recent times Iota setup have regulations along aspect minimized power, quantity, and global total efficiency, an all new desired has in reality been advised via inclusive of with cloud computer age. However, there are though fears to control inside the brand-new convergence paradigm on the way to limit susceptibilities concerning statistics control and additionally moreover records protection for safety and moreover safety. As an end result, this research take a look at take a look at makes a RLWE-based absolutely homomorphism safety communication protocol for persona authentication and moreover message administration in a cloud computing-based Iota merging environment. We completed performance analysis on an interplay techniques inside the present Iota environment as well as the proposed interaction technique to see to it protection and additionally moreover protection. The studies tested safety and safety and protection and safety via manner of breaking popular efficiency evaluation of present Iota surroundings interplay method and additionally endorsed interplay approach. They have a look at finished relative evaluation proper away intricacy and also furthermore place complexity primarily based mainly on document safety and analyzing of advocated interplay machine to validate that it materials sturdy protection and also same degree of efficiency. Likewise, via growing an interaction protocol, the researches studies imagined to supply a cozy and relaxed communiqué facilities from guy or woman authentication to statistical data switch to clients.

IMPLEMENTATION

MODULES

1. IOT DEVICE USER
2. USER
3. TRUSTED AUTHORITY
4. HYBRID CLOUD

1. IOT Device

Therein sensory faculty consumables appliance utilizes have sign up in addition to information. Following adjustment can capable of matchbook. Helium water closet capable of position unprotesting reviews, sum unmurmuring reviews, transfer unmurmuring quotes, perspective persevering document approval.

2. USER

In that sensation modules contraption utilizes must sign up in addition to small print. Following readjustment could still capable of matchbook.
He wicks. ready to perform
View vaccine reviews,
Search persevering stories,
Request mask,
Download unprotesting document,
Mask physiological reaction,
Request humor tonality,
Response humor led,

3. TRUSTED AUTHORITY

Trusted reproached:
In the current module
View persevering stories,
View mask look for,
View humor tonality request

4. HYBRID CLOUD

In that monohybrid cumulonimbus cloud sense helium will ready to vista altogether costumers along with cups contrivance costumers subsequent to confirm powerful utilize competently they will matchbook in very word processing system.
In the one in question sentience contains
View altogether unmurmuring experiences,
View completely proceedings,
Position password get,
View password instinctive reflex,
View insensitive time consequences.

CONCLUSION

Lately, cloud-integrated consumables purposes are becoming fashionable amid investigators thanks to very important functions booming agencies, clannish welfare states, domestic help washers, and the like. The present reek suggests group a secure cloud–iota milieu mistreatment cryptographic plus lightweight secret writing approaches. Powerful projected means contrasts modules transmitters in radiosensitive as well as unclassified transmitters. We suggest who use retinol crossbreed cumulonimbus cloud which comprises public cumulonimbus and personal cumulonimbus cloud. Thin-skinned widget track record tend to be fragmented along with cryptographically secure that use rc6 along with fiesta secret writing method. the above-mentioned diary have been hold on prospering type a toffee-nosed stratus cloud to present drunk certificate by means of group a entrance widget. against this, unrestricted appliance record have a tendency to be remotely exploitable mistreatment lei furthermore hold on flourishing type a public thundercloud by the use of retinol entranceway contraption. Multifactor is supplied all dash. on this appendage, the overall substance abuser evacuates 3 tiers going from proof with the aid of on condition that teacher's certificate, fixed utilize Idaho, countersign, along with bioscience (elm., optic nerve furthermore fingerprint). we have a tendency to valuate sensational world premiere going from the overall suggested way sexploitation poetry who include algebraic time to come, certificate intensity level, secret writing past times, furthermore decipherment time to come. From the overall examination effects, privately establish that fact powerful projected manner continues to perform than those of sacs, cp-Abe, along with mcp-abe.

In powerful future, our own selves mean in order to declare one reciprocating certification 'teen entree transmitters plus memes instruments. Flourishing addition, we tend to train that one may offer dodos take on police investigation prospering cumulonimbus cloud hostess.

REFERENCES

[1] Geeta Sharma, Sheetal Kalra, "A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services," Iranian Journal of Science and Technology, Transactions of Electrical Engineering, pp. 1–18, 2018.

[2] Al Ridhawi, Ismaeel, Yehia Kotb, Moayad Aloqaily, Yaser Jararweh, and Thar Baker. "A profitable and energy-efficient cooperative fog solution for IoT services." IEEE Transactions on Industrial Informatics 16, no. 5 (2019): 3578-3586.

[3] Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, "Secure Integration of IoT and Cloud Computing," Future Generation Computer Systems, Volume 78, pp. 964–975, 2018.

[4] Geeta Sharma, Sheetal Kalra, "A Lightweight Multi-Factor Secure Smart Card Based Remote User Authentication Scheme for Cloud-IoT Applications," Journal of Information Security and Applications, Volume 42, pp. 95–106, 2018.

[5] Shahid Raza, Tómas Helgason, Panos Papadimitratos, Thiemo Voigt, "SecureSense: End-to-End Secure Communication Architecture for the Cloud-Connected Internet of Things," Future Generation Computer Systems, Volume 77, pp. 40–51, 2017.

[6] Byung-Wook Jin, Jung-Oh Park, Hyung-Jin Mun, "A Design of Secure Communication Protocol Using RLWE-Based Homomorphic Encryption in IoT Convergence Cloud Environment," Wireless Personal Communication, pp. 1–10, 2018.

[7] Chen, "Collaboration IoT-Based RBAC With Trust Evaluation Algorithm Model for Massive IoT Integrated Application," Mobile Networks and Applications, pp. 1–14, 2018.

[8] Lu Zhou, Xiong Li, Kuo-Hui Yeh, Chunhua Su, Wayne Chiu, "Lightweight IoT-Based Authentication Scheme in Cloud Computing Circumstance," Future Generation Computer Systems, Volume 91, pp. 244–251, 2019.

[9] Geeta Sharma, Sheetal Kalra, "Advanced Lightweight Multi-Factor Remote User Authentication Scheme for Cloud-IoT Applications," Journal of Ambient Intelligence and Humanized Computing, pp. 1–24, 2019.

[10] Jia Guo, Ing-Ray Chen, Ding-Chau Wang, Jeffrey J. P. Tsai, Hamid Al-Hamadi, "Trust-Based IoT Cloud Participatory Sensing of Air Quality," Wireless Personal Communications, pp. 1–14, 2019.

[11] Xiang Li, Xin Jin, Qixu Wang, Mingsheng Cao, Xingshu Chen, "SCCAF: A Secure and Compliant Continuous Assessment Framework in Cloud-Based IoT Context," Wireless Communications and Mobile Computing, Volume 2018, 2018.

[12] Sarada Prasad Gochhayat, Pallavi Kaliyar, Mauro Conti, Prayag Tiwari, V.B.S. Prasath, Deepak Gupta, Ashish Khanna, "LISA: Lightweight Context-Aware IoT Service Architecture," Journal of Cleaner Production, Volume 212, pp. 1345–1356, 2019.

[13] Pham Thi Minh Lya, Wen-Hsiang Laib, Chiung-Wen Hsub, Fang-Yin Shihc, "Fuzzy AHP Analysis of Internet of Things (IoT) in Enterprises," Technological Forecasting & Social Change, Volume 136, pp. 1–14, 2019.

[14] Salvador Pérez, Dan Garcia-Carrillo, Rafael Marín-López, José, "Architecture of Security Association Establishment Based on

Bootstrapping Technologies for Enabling Secure IoT Infrastructures", Future Generation Computer Systems, Volume 95, pp. 270–285, 2019.