Neoteric Security and Privacy Sanctuary Technologies in Smart Cities

Chinkit Manchanda[1], Nikhil Sharma[1*], Rajat Rathi[1], Bharat Bhushan[1], Moksh Grover[1]
[1]HMR Institute of Technology & Management, Delhi, India
{chinkitm51,nikhilsharma1694,rajatrathi25, mokshmg}@gmail.com
bharat_bhushan1989@yahoo.com

***Abstract*—A Smart city is an area that practice several kinds of automated Internet of Things (IoT) sensors to gather information and then make efficient use of perceptions acquired from that information to organize resources, services and assets proficiently. The primary purpose of Smart cities was to refine and enhance the life style of the people, encourage development without affecting the resources for the future generations and advancement of the functionalities in urban areas. With the rapid acceleration in the development of smart devices, security and privacy problems have turn out to be a main task that needs efficacious counter actions. Majorly, this survey commences with an outline of smart cities to offer a cohesive framework. After that, there is discussion about the privacy and security problems in present smart systems through the various necessities for making of a steady and safe smart city. To conclude, we review the present security techniques and as well inspirit others to further research more this evolving ground.**

Keywords-Internet of Things(IoT), security, privacy, Blockchain, Cryptography, Game Theory.

I. INTRODUCTION

There is no globally recognized definition to the question "What is a smart city?". It varies from people to people. This concept, therefore, differs from state to state and from country to country. Every government on the globe understands and works for smarter cities in different ways. Even in one country, say India, there is not one definition to 'Smart cities. The reason for this definition to vary is dependent on the fact that no state or no country is alike, every state in every country has its own potential, carry a pace of development and different requirements. A smart city is generally a wish list of the services and infrastructural development according to the country's scope of development and requirement of the development. To fulfil the needs of the people, the state developers plan to develop the whole urban eco-system, which rely further on four pillars of development in the fields of – institutional, physical, social and economic infrastructure. This together works in incrementing the level of 'smartness' of cities.

This conception of smart cities has managed to grab the attention of both the people and the industries because of the increasing urban advancement and infrastructural growth. According to recent reports, it is estimated that around 66 percent of the total population of the world will start to live in the urban surroundings by the year 2050 [1], that may result in burdening the environment and lead to climatic and environmental degradation. To solve this problem, different governments are aiming at development of the smart cities in an intelligent and sustainable way. Cisco has announced the investment of one billion dollars for the growth of smart cities, China also has around 200 smart city plans in implementation [2]. In Figure 1, it shows security is being increased at every level by the IoT services in their devices.

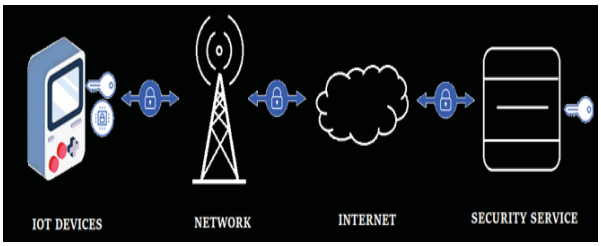

Figure 1. Security Levels of IoT devices

The development of 'smart things' being deployed in the smart cities is increasing rapidly and so are the range of susceptibilities that can be used for the exploitation of people by cyber criminals. Though development of smart cities focuses on the rise of productivity and efficiency, but they can be vulnerable spots for serious risks for people when the cyber security is not taken care of properly. These are some common attacks and their countermeasures adapted till now:

- The middle man attack: In this kind of attacks, a person breaches and attempts to interrupt the connection or communications between two systems. For example, these men can breach into the smart locks of the houses and cause burglary or other crimes. These are controlled by using proper authentication and double encryptions.
- Fake identity attack: The EV charging stations, camera for surveillance and the parking garages are some of the smart city infrastructures which are unprotected and the data generated from these can be used as a fuel to the cyber attackers providing confidential private information that can be used for frauds or identity theft. These are prevented by Authentication, encryption and managing access controls.
- Device hacking: In this kind of attack, the attacker hacks the device and takes over the control of the device and further use the device for personal benefits without regarding the privacy of the initial owner and attempts to exploit the privacy of the

978-1-7281-4976-9/20/$31.00 ©2020 IEEE
DOI: 10.1109/CSNT.2020.44

owner. These kinds of attacks are more reportedly occurring than the others and many attempts are being made for controlling and minimizing such risks. Strong device identification and concerned access controls are provided to the users for prevention.

This paper aims at providing a reality check to the audience about the security and privacy concerns in the IoT devices equipped smart cities. These cities are well equipped to provide luxury to the people and therefore attract large number of people and industries to it but a negative aspect which is not so much enlightened are the security threats and risks, this technology brings along. This paper also focusses on the challenges faced by the technology in solving these security issues and the threats it offers to the mankind.

II. Architecture of Internet of Things for Smart Cities

By the pace of growth of smart cities and to compete with pace, several architectures have been introduced [3]. There is a lack of uniformity in these IoT architectures. As per the purpose of this study is to review safety and privacy problems in smart cities. The following planning is built on three-layer architecture proposed et al K. Angrishi [4]. The architecture consists of layers described briefly below, as shown in Figure 2.

- **Perception Layer:** This is the physical layer, as well identified as the sensing layer, which has sensors for sensing and collecting data. It's the lowest layer in the architecture. The primary objective of the perception layer in IoT is to gather information, the security challenges in this layer emphasis on the imitating gathered information and terminating perception devices.
- **Network Layer:** This is the layer accountable for connecting to other smart devices, networks, and servers. It identifies itself as the core layer of the IoT architecture which rely on simple links. Its characteristics are used for transmission of information gathered from the perception layer and processing sensor information.
- **Support Layer:** This layer works hand-in-hand with the application layer and providing support to the necessities of various applications via smart computing methods.
- **Application Layer:** It is uppermost layer in the architecture joining from client side. It provides an interface between the end devices and the complete system. It is responsible for delivering specific services required by applications based on user requirements.

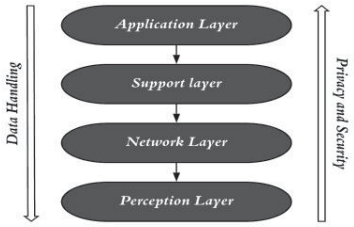

Figure 2. Architecture of IoT for Smart Cities

III. Applications of IoT in Smart Cities

The idea to create devices smart enough to decrease man work to nearly nil. The concept of interlinked devices where the technology is smart enough to exchange data with us, to cloud based technology and to each other (device to device). The illustration of the emerging smart applications of smart cities [5] are described below in Figure 3.

A. Smart Homes

Smart home devices, also often stated to as homebased mechanization. It is the residential extension of building automation and comprises the control and automation of all its embedded technology. A smart home is one in which the several electric and electronic appliances are connected to a central computer control system so they can be controlled by the user easily through some application like either be switched on and off at certain times. Smart home offers, security, energy efficiency, small functioning expenses and suitability. Installation of smart appliances deliver ease and save time, money and energy.[6]

B. Connected Cars

The Internet of things breakthrough the grounds of car industry by presenting completely new layers to the traditional method of cars. Connected car technology depend on a wide network of sensors, antennas, embedded software, and communication technologies to steer in our multiplex world. It has to make sensible choices with precision, momentum and reliability.[7] These necessities will become even more hypercritical when people renounce control of the steering wheel and brakes to the self-directed automobiles that are being positively tested on our highways now.

C. Smart Farming

Smart farming is an evolving idea that signifies to managing fields using technologies like IoT, robotics, drones and AI to increase the production and quality of crops while improving the human labour required by production. It can be done by monitoring the crop growth using digital sources. This will offer the precise values of several constraints upon which the growth depends. It will help the agriculturalist to monitor more than one agricultural field at the same period. Growth in business productivity by procedure automation. By the use of smart devices, you can systematize several procedures across your process of production, e.g. pest control, irrigation, or fertilizing.[8] There is a smart

agriculture sensors equipped product known as GreenIQ which is fascinating product. that uses smart agriculture sensors. It is a smart sprinklers regulator that lets you to achieve your irrigation and lighting systems remotely.

D. Smart Environment

Two things determine the building and process of smart cities: gathering information from the environment and permitting individuals to use that information in a productive manner—sometimes to change behaviour.[9] Smart environments goal to gratify the involvement of individuals from every environment, by substituting the harmful labor, physical labor, and tedious jobs with automated agents. By implementing technical supervision gears, smart environment has potential to keep track of energy consumption, air quality, traffic congestion and bring the pollution and waste rate in consideration [10].

E. Smart Industry

This Smart Industry tendency is fetching about an essential alteration in the technique factories and workplaces work, to make them secure, more effective, more versatile and more nature friendly. The Industrial IoT is the root for the Industries, which mentions universally to bring automation and data exchange into the practice for manufacturing, also using robotics, system integration, cybersecurity, the Cloud, data analytics, and augmented reality. These methods are defined to make a "smart factory" where machineries, systems, and people communicate with each other in accordance to manage and observe development along the assembly line.[11]

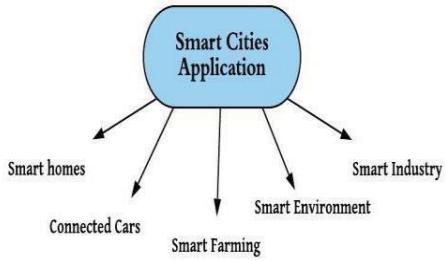

Figure 3. Applications of Smart Cities

IV. Security and Privacy Issues in Smart Cities

In a smart city, the data produced by people living there over years could well be far more treasured than the property on which they are living. If information is not effectively protected and privacy is not promised, smart cities could change from user-centric vision into groups that pose substantial danger. In past years, some issues have been found in various execution situations. For example, in the framework of smart homes and healthcare, smart machine producers and facility providers might get their hands on the private information [12]. Some of the newest problems caused by the swiftly evolving smart applications are listed below.

A. Botnet Threats

A botnet can be described as a group of internet-based applications, which includes computers, servers and Internet of Thing (IoT) machines contaminated and succeeded by a mutual kind of attacks, such as Denial of Service (DoS), DDoS, phishing outbreaks [13]. Bots distinguish from common malware, in which they consist of a network of commute with their makers, permitting them to give instructions to their system of bots (i.e., Zombies) and thus creating botnets multipurpose when it comes to their usage [9][10].

B. Autonomous Cars as a Threat

Self-driven cars are the future of transportation, these advanced automobiles are potentially vulnerable to an entire multitude of security problems. This swiftly developing technique has been realized as a foremost safety problem as when an AV is hacked, both life protection and information security will be in jeopardy.[14] Explicitly, hackers can manipulate the safety to govern remotely controlled strikes.

C. Security vulnerabilities in smart cities

The main fears concerning smart cities and the people living there is that the gears and the instruments that transmit information which can be hacked with no trouble. The hacker can then access the private information of the users and cause application collapse, can cause all kinds of wide scale signal loss, such as shutting down of tunnels or vaccinating toxins into the main water source.[15]

D. Artificial Intelligence threats

Artificial intelligence devices show crucial parts in numerous smart applications, such as automated customer support, personalized shopping experience, etc. Nevertheless, the increasing usage of Artificial Intelligence also constitute some security risks.[16] For an instance, Self-governing weaponries are AI systems that are automated to slaughter. In the hands of the wrong individual, these weaponries could simply cause mass casualties.

V. Security Requirements

IoT security is the technology zone apprehensive with protecting linked devices and grids in the internet of things (IoT). Permitting systems to link to the internet unlocks them to numerous of significant vulnerabilities if they are not correctly secured.[17] Therefore, IoT security assists maintaining information integrity and preventing information by hackers. All transmission with your IoT applications should be validated using powerful password, validation protocols or time-based validation tokens.[18]

A. Validation and Privacy

Validation is a primary prerequisite for secure implementation of a smart system and is desirable to demonstrate characteristics and guarantee the clients with authorization can acquire facilities across an assorted scheme [19]. Explicitly, IoT machines installed in smart cities can validate the system, other junctions, and the communications from administration.

B. Key Functional Blocks

IoT safekeeping solutions require to execute the functional blocks explained below as interrelated parts, not in separation, to reach the IoT measure, information safety and device trust.[20]

a) *Device Reliance:* Creating and handling Device Distinctiveness and Veracity.
b) *Information Safekeeping:* Strategy determined end-to-end information safety, confidentiality from conception to feasting.
c) *Operationalizing the Assurance:* Systematizing and interfacing to the ideal based build, verified machineries.

C. Lightweight invasion recognition and forecasting

To discovering a security community to share risk intellect and hardening resources, a smart system is considered to be safe only if it can monitor the complete process and keep record of timely events and to notice any kind of unusual actions in an any event. The intrusion detection system (IDS) is extensively used in monitoring.[21] An IDS helps in safety like firewalls and antivirus to frequently analyze network traffic compared to known malicious movements.

VI. Current Security and Privacy Protection Technologies

This segment highlights the present and important technologies used to manage safety and privacy dreads in the smart cities.[22]

A. CRYPTOGRAPHY

Cryptography is a very essential technology which is used for safeguarding the information that travels over the WWW. Encryption is used to prevent the content of the emails, newsletters, chats, calls, web transactions and different forms of media shared over the internet from being stolen and mishandled. Cryptography makes sure to fulfil its role in providing authentication, authorization, confidentiality, integrity and nonrepudiation of the information to the author. Cryptographic algorithms play a vital role in jobs such as data encryption, digital signatures. The public key infrastructure systems (PKIS) are used for designing the cryptographic keys that encrypt the data transient among the useful characteristics like email addresses, domain name system addresses, etc. The cryptographic algorithms are now being used in an incrementing ratio of devices to ensure high security. In the IoT field, cryptographic algorithms are the majorly used privacy protection methods allowing a large number of tools to be applied practically.

The old-style algorithms and encryption methods are not much fit for the high technology-based devices used now because of the increased complexity levels and varying energy consumption requirements. In this way the lightweight encryption methods comes to limelight and used for applying the cryptographic technologies. For the protection of users' communication from both ends from the DDoS attacks. Mahmood et al introduced a lightweight authentication mechanism that targets to provide safety to the smart city applications.

Another method that has attained increasing importance in the past years is Homomorphic encryption (HE) that performs calculations on the encrypted data. The homomorphic encryption method focusses on preventing the sensitive information from being decoded while performing the calculations.

Zero-knowledge proof is one of the more improved cryptographic method that allows one group to substantiate something to the other parties, without revealing the encrypted data. For example, Dousti et al. [23] developed an authentication protocol using zero-knowledge proofs for smart cards.

B. BLOCKCHAIN

Blockchain at a very basic level can be called as a chain of blocks but not technically. The word "block" actually refers to the digital information and the word "chain" is referring to the database in which it is stored. This database is public.[24] The digital information mainly comprises of three parts: i) These blocks stores information about your transactions like the time, date, and amount of the most recent transaction in dollars. ii) blocks store information about the participant in the transaction in the form of the digital signature which acts as a unique username. iii) lastly, they store data that is used to differentiate it from other blocks by using a unique 'hash' code, which are cryptographic codes created using cryptographic algorithms. For new data to be added to the Blockchain, four steps have to happen, that are: i) a transaction must take place, ii) the same transaction must be verified, iii) that transaction must be stored in a block, iv) a unique hash code must be given to the block.

A copy of every Blockchain is available to all the computers in the network and all the copies are identical to one another, that makes the manipulation of the information very difficult. So, for manipulation of one piece of information, the hacker would need to manipulate all the copies of a particular Blockchain on the network. Therefore, Blockchain is also termed as "distributed ledger".

This clearly increases the reliability of users on the Blockchain for multiple applications' security, but it is still primary stage in the field of IoT.

C. BIOMETRICS

Biometrics is one of the most used authentication techniques used in the IoT based systems. Biometrics are the physical human characteristics which digitally identify a person to provide access to devices or systems or data. Facial patterns, voice and fingerprints are the mostly used biometric identifiers. Biometrics have potential to secure devices and data more effectively than other techniques and methods. According to recent studies, biometrics are ranked as 'effective' and 'very effective' for securing data and protecting the data stored in cloud.

For biometric techniques to be effective, the implementation, maintenance and usage of these techniques should be proper, otherwise the risk of leakage of data can increase.

D. MACHINE LEARNING AND DATA MINING

Machine Learning is like making the computers learn without being particularly programmed. The ability to learn makes the computers much like humans. Machine learning has been a great success in detecting intrusions which helps in protecting the networks from attacks to a great extent. The WSNs (Wireless sensor networks) have become an essential element in this smart arena. Machine learning focuses on the development computer programs that uses the data to learn and train themselves for similar data predictions.

Data mining is phenomenon that transforms the raw data into important information, generally used by companies. It helps in the development of business by learning more about their customers. Data mining helps in the development of more effective strategies of marketing, increase sales and decrease costs. Data mining involves the exploration and analysis of data to gather possible patterns and inclinations.

E. GAME THEORY

Game theory is now an emerging powerful tool that is successfully applied in the cybersecurity fields and security domain of smart homes. Game theory is the study of mathematical models of calculated communications between the rational decision makers. Its applications are used in all the fields of logical and computer science.

John von Neumann gave the proofs for the modern game theory using the zero-sum games. Many mechanisms have been developed from various studies by linking game theory with other security and protection of privacy-based technologies, like differential privacy. Moreover, game theory is also a powerful mechanism to maintain the protection intensity and utilization of the data. Although game theory is not much implemented by studies and not much applications are present in this technology, major development is yet in the field IoT security. But hopes for game theory to develop and be more improved and implemented in the smart world are high.

VII. CHALLENGES FACED BY IOT IN SMART CITIES

We are now living in a reality that was just an imagination once and all thanks to the Internet of Things (IoT) for it. It is IoT which developed the concept of smart cities and fulfilled it and brought the world to this stage. Obviously, it was not an easy journey. It faced many challenges and is still facing more as the technology grows.[25] Some of the challenges are mentioned here:

- **Infrastructure:** Smart cities use sensors for information gathering, analysis and utilization of other types of energy resources. It is already very difficult to remove all the old hard-wired infrastructure with the new sensor based wireless infrastructure. Along with that, the security of the devices is also to be maintained using these sensors. Internet is considered to be fault resistant but one breach in the network can lead to interruption in the privacy of all the connected devices.
- **Driverless Car threats:** The autonomous vehicles are stealing all the attention these days. They are being worked upon for reducing the traffic accident rates and to build a smarter society. But they can be proved to be very risky if the AVs (autonomous vehicles) are hacked. The hackers can threaten the life inside and outside the vehicle at ease.
- **Household appliances:** The smart devices have reduced the privacy of the houses even more. There is no house now with no smart devices in any room, be it kitchen, living rooms, garages, or the bedrooms. These devices are of great help but once hacked can be fatal. The mobile phones if hacked can use cameras and exploit the privacy of people, the smoke sensors in houses or the microphones in the televisions can also be hacked.

TABLE I. THREATS AND COUNTERMEASURES OF IOT IN SMART CITIES[26,27]

Serial No.	*Threats*	*Countermeasures*
1.	**Privacy and Identity theft**	Authentication, Encryption and Access Control
2.	**Device Hacking**	Device Identification and Access Control, Security Lifecycle Management
3.	**Permanent Denial of Service (PDoS)**	Authentication, Encryption, Access Control and Application Level DDoS Protection, Security Monitoring and Analysis
4.	**Application Level Distributed Denial of Service (DDoS)**	Device Identification and Access Control, Security Monitoring and Analysis
5.	**Middle Man Attack**	Authentication and Encryption, Security Lifecycle Management

To solve such issues, more and more money and minds are invested to come up with better and safer devices with are more trustable and adaptable in people's lives to protect users against hacking and cyber-crimes. Better and stronger encryption techniques are used to increase the security in new applications of IoT brought into the world of smart cities.

VIII. CONCLUSION

The extensive usage of smart devices has induced several safety and privacy problems. The growth of more innovative safety models is important and vastly required in both business and educational domain. Inspired by these reasons, we surveyed the modern strategies and developments in corresponding actions from the perceptions of several plans. To find the solution for the security issues for the swiftly emerging smart devices, it is rational to forecast that in the succeeding years, alleviating the existing problems will be the prime responsibility of smart city associated studies.

REFERENCES

[1] Y. Li, Y. Lin, and S. Geertman, “The development of smart cities in china,” in Proc. of the 14th International Conference on Computers in Urban Planning and Urban Management, 2015, pp. 7–10.

[2] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani, “Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges,” IEEE wireless communications, vol. 24, no. 3, pp. 10–16, 2017.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” IEEE Internet of Things journal, vol. 1, no. 1, pp. 22–32, 2014.

[4] K. Angrishi, “Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets,” arXiv preprint arXiv:1702.03681, 2017.

[5] L. Tan and N. Wang, “Future internet: The internet of things,” in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, vol. 5. IEEE, 2010, pp. V5–376.

[6] Soni, S., & Bhushan, B. (2019). Use of Machine Learning algorithms for designing efficient cyber security solutions. *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. doi: 10.1109/icicict46008.2019.8993253

[7] Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T. and Rossow, C., 2015. “IoTPOT: analysing the rise of IoT compromises.” EMU, 9, p.1.

[8] Pijpker, Jeroen, and Harald Vranken (2016) "The role of Internet Service Providers in botnet mitigation." Intelligence and Security Informatics Conference (EISIC), 2016 European. IEEE.

[9] Silva, S. S. C.; Silva, R. M. P.; Pinto, R. C. G. & Salles, R. M. (2013), 'Botnets: A survey', Computer Networks 57(2), 378 - 403.

[10] Khattak, S.; Ramay, N. R.; Khan, K. R.; Syed, A. A. & Khayam, S. A. (2014), 'A Taxonomy of Botnet Behavior, Detection, and Defense', IEEE Communications Surveys Tutorials 16(2), 898-924.

[11] M. Chiang and T. Zhang, “Fog and iot: An overview of research opportunities,” IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854–864, 2016.

[12] Sinha, P., Jha, V. K., Rai, A. K., & Bhushan, B. (2017). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. *2017 International Conference on Signal Processing and Communication (ICSPC)*. DOI: 10.1109/cspc.2017.8305855

[13] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, “Anonymous authentication for wireless body area networks with provable security,” IEEE Systems Journal, 2016.

[14] A. Abduvaliyev, A.-S. K. Pathan, J. Zhou, R. Roman, and W.-C. Wong, “On the vital areas of intrusion detection systems in wireless sensor networks,” IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1223–1237, 2013.

[15] Khamparia, A., Singh, A., Anand, D., Gupta, D., Khanna, A., Kumar, N. A., & Tan, J. (2018). A novel deep learning-based multi-model ensemble method for the prediction of neuromuscular disorders. *Neural Computing and Applications*. doi: 10.1007/s00521-018-3896-0

[16] Jaitly, S., Malhotra, H., & Bhushan, B. (2017). Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor Networks: A survey. *2017 International Conference on Computer, Communications and Electronics (Comptelix)*. DOI: 10.1109/comptelix.2017.8004033

[17] Q. Jing, A. V. Vasilakos, J.Wan, J. Lu, and D. Qiu, “Security of the internet of things: Perspectives and challenges,” Wireless Networks, vol. 20, no. 8, pp. 2481–2501, 2014.

[18] Z. Mahmood, H. Ning, and A. Ghafoor, “Lightweight two-level session key management for end user authentication in internet of things,” in Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on. IEEE, 2016, pp. 323–327.

[19] Saini, H., Bhushan, B., Arora, A., & Kaur, A. (2019). Security vulnerabilities in Information communication technology: Blockchain to the rescue (A survey on Blockchain Technology). *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. doi: 10.1109/icicict46008.2019.8993229

[20] M. Kearns, M. Pai, A. Roth, and J. Ullman, “Mechanism design in large games: Incentives and privacy,” in Proceedings of the 5th conference on Innovations in theoretical computer science. ACM, 2014, pp. 403–410.

[21] Kaushik, I., Sharma, N., & Singh, N. (2019). Intrusion Detection and Security System for Blackhole Attack. *2019 2nd International Conference on Signal Processing and Communication (ICSPC)*. doi: 10.1109/icspc46172.2019.8976797

[22] O.-J. Lee, H. L. Nguyen, J. E. Jung, T.-W. Um, and H.-W. Lee, “Towards ontological approach on trust-aware ambient services,” IEEE Access, vol. 5, pp. 1589–1599, 2017

[23] M. S. Dousti and R. Jalili, “An efficient statistical zero-knowledge authentication protocol for smart cards,” International Journal of Computer Mathematics, vol. 93, no. 3, pp. 453–481, 2016.

[24] Varshney, T., Sharma, N., Kaushik, I., & Bhushan, B. (2019). Authentication & Encryption Based Security Services in Blockchain Technology. *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. doi: 10.1109/icccis48478.2019.8974500

[25] G. Xu, Y. Cao, Y. Ren, X. Li, and Z. Feng, “Network security situation awareness based on semantic ontology and user-defined rules for internet of things,” IEEE Access, vol. 5, pp. 21 046–21 056, 2017.

[26] W. Hurst, N. Shone, A. El Rhalibi, A. Happe, B. Kotze, and B. Duncan, “Advancing the micro-ci testbed for iot cyber-security research and education,” CLOUD COMPUTING 2017, p. 139, 2017.

[27] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, “Privacy-by-design framework for assessing internet of things applications and platforms,” in Proceedings of the 6th International Conference on the Internet of Things. ACM, 2016, pp. 83–92.