Tec Empresarial
P-ISSN: 1659-2395; E-ISSN: 1659-3359

DISASTER PROTECTION OF EXECUTIVES FRAMEWORK FOR INDIVIDUALS TO EMPTY FROM CALAMITY AREA.

***Note: Sub-titles are not captured in Xplore and should not be used**

Haritha Prabhakaran
Department of Information Technology, Panimalar Engineering College, Chennai, India
haritha81997@gmail.com

Maria Princi Arulsamy
Department of Information Technology, Panimalar Engineering College, Chennai, India
mariaprinci22@gmail.com

Renitha Selvaraji
Department of Information Technology, Panimalar Engineering College, Chennai, India
renithaselvaraji@gmail.com

Devika Manjunath
Department of Information Technology, Panimalar Engineering College, Chennai, India
devikamanjunathhosur@gmail.com

Abstract— The management of disasters, which can be man-made or natural, entails how we respond to their effects. It's the process of preparing for, managing, and learning from major failures. Prompt and well-thought-out evacuation procedures are crucial to guaranteeing people's safety when calamities hit. Before any preventative steps are required to stop future disasters in that area, people depart the disaster area. At the time, individuals had to assist that area during the occasional floods. The proposed framework aims to give catastrophe management and efficient evacuation operations a useful and user-friendly platform. One important role that the "Rescue People" module plays in aiding disaster victims and ensuring timely evacuation is allowing qualified persons and volunteers to register and participate in rescue missions. The "Government" module allows crisis management authorities to plan rescue operations, provide resources, and keep an eye on data in real-time. For those who find themselves stranded in disaster-affected areas, there is a module called "Disaster Victims." They can request assistance, receive updates, and acquire vital evacuation information via the app. Thanks to centralized control, administrators may maintain user accounts and ensure the smooth operation of the framework with the aid of the "Admin" module. Additionally, rain data is scraped from websites that offer weather forecasts to enhance the design. This comprehensive method combines human and technical resources to manage and efficiently respond to disasters. It emphasizes the importance of community involvement, timely information, and cooperation in ensuring everyone's safety.

Keywords— AES encryption, Authentication, AES encryption, Disaster protection, emergency response, emergency alert, HAS 256,post-disaster situation awareness, security, resource demand.

I. INTRODUCTION

Whether a disaster is caused by human activity or natural causes, disaster management is an essential procedure for handling its aftermath. It entails foreseeing probable catastrophic errors, acting upon them, and learning from them. Disaster management requires the rapid and organized implementation of evacuation measures, particularly in situations when there is a significant chance of human casualties. The recommended architecture aims to develop an efficient and user-friendly platform for evacuation operations and overall disaster management. Numerous modules that are designed to assist specific tasks and duties make up the structure. The "Rescue People" module is designed for trained individuals and volunteers who are willing to sign up and participate in rescue operations. Their involvement is crucial to assisting catastrophe victims and ensuring a prompt and efficient evacuation procedure. The agencies in charge of managing catastrophes are intended to use the "Government" module. Thanks to this module, they may plan the strategic deployment of necessary resources, manage rescue operations, and monitor real-time data. People who are left behind in areas devastated by disasters are the focus of another lesson called "Disaster Victims." Thanks to this module, they can seek assistance, receive timely updates, and obtain important information regarding their evacuation. The "Admin" module offers centralized control over the entire system. Administrators may manage user credentials, monitor system performance, and ensure smooth operation with this module. To collect rain data, the framework also contains web scraping of websites that provide weather forecasts. These statistics increase the overall efficacy of the system. This comprehensive approach integrates technical and human resources to efficiently handle and address crises. It highlights the significance of community engagement, timely information exchange, and cooperation in ensuring everyone's safety. Through the promotion of a proactive and collaborative approach to disaster management, the framework serves as an adaptable tool to tackle the various challenges presented by natural disasters.

A. PROBLEM STATEMENT

1) Security in Disaster Areas: Disaster-stricken areas are vulnerable to various types of cyber attacks and malicious activities that can disrupt data sharing and compromise the reliability of the information exchanged within the disaster environment.

2) Ensuring the integrity and immutability of data transactions is crucial for disaster rescue operations. Existing centralized systems may not provide the necessary level of trust and reliability.

B. OBJECTIVES

- The information sharing and compromise of the dependability of the data traded inside the disaster area.
- The information-sharing structure should be productive as far as accomplishing agreement among network hubs to overcome this we make a cloud-based structure.

II. RELATED WORK

Disaster management relies heavily on information sharing, but it can be challenging due to potential flaws in the accuracy of shared data in disaster-affected areas. To solve this issue, a cohesive information-sharing structure that aims to bring network nodes together is required. Putting in place a cloud-based infrastructure is one innovative solution.

Put another way, effective communication and the sharing of critical information are essential during times of disaster. But in a chaotic crisis scenario, it might be very challenging to protect the integrity of shared data. Traditional information-sharing networks may be disrupted by hackers or other factors, making coordinated disaster response difficult.

A cloud-based approach is proposed to address these issues. Consider this building as a cloud-based disaster management environment, similar to the cloud storage we use for documents and photos. With this cloud-based architecture, multiple parties—including affected individuals, governmental organizations, and emergency responders—can safely exchange and access real-time data.

A cloud-based strategy's primary advantage is its ability to persuade network nodes to cooperate. Stated differently, it streamlines the process of reaching consensus. It is imperative to have a system in place that enables reliable and timely information sharing during emergencies since every second counts.

Consider this cloud-based infrastructure as an authorized user-only central store for all relevant disaster-related data. Emergency responders may readily obtain real-time updates, maps, and evacuation schedules. Governmental authorities possess the ability to monitor developments, provide resources, and take prompt, decisive action. Even individuals who are impacted can find essential evacuation information, ask for assistance, and receive updates thanks to technology.

By utilizing cloud technology, the system also ensures data integrity and confidentiality. It reduces the likelihood of data compromise and increases the general dependability of shared information. This cloud-based information-sharing architecture becomes a useful tool for disaster relief, promoting a reliable, efficient, and well-coordinated response to mitigate the impact of disasters on affected communities. It modifies the way information is shared during crises, which contributes to a more effective and coordinated disaster management procedure.

A. Tables

No of events	350
No people were killed	52,000
Average killed per year	433.33
No of the people affected	10 million
Average affected per year	833,333,33
Economic damage(US$ X 1,000)	$15 billion
Economic Damage per year(US$ X 1,000)	$1.25 billion

TABLE I NATURAL DISASTERS FROM 1980-2023

TABLE II MAN-MADE DISASTERS FROM 1980-2023

Date	Disaster	Location	No.of People Death
2018-06-07	Building Collapse	Mumbai, Maharashtra	23
2018-08-19	Train Derailment	Uttar Pradesh	23
2019-05-24	Cyclone Fani	Odisha	64
2019-09-07	Boat Capsizing	Andhra Pradesh	12
2020-05-07	Gas Leak	Visakhapatnam, Andhra Pradesh	12

III. LITERATURE REVIEW

The application of tactics to lessen a disaster's harmful effects is the aim of disaster management. The usage of mobile applications and artificial intelligence (AI) is considered to play a crucial role in disaster mitigation, planning, response, and recovery with the recent breakthroughs in technology. Therefore, an architecture for intelligent catastrophe management for the Philippines, a developing nation, is suggested in this study. Conversely, the adoption of the created mobile application for simulating catastrophe preparedness is assessed in this paper. The potential of system architecture for disaster preparedness is confirmed by this study, which helps create decision intelligence for disaster management. This study is among the few that aim to illustrate an intelligent disaster management architecture in a developing nation to support the creation of policies and practices.[1][5]

Instead of emphasizing the publications' metrics, the methodology concentrates on the articles' substance and the study itself., even if more material regarding local ride-sharing systems may exist in different languages. A major problem for many cities, including Jakarta, has been flooding because of the city's location, climate, and population habits. One of the Sustainable Development Goals, according to the UN, is catastrophe management. Nevertheless, the implementation of complete flood management services remains a difficulty for many towns in developing countries. In this study, we elaborate on efforts that have been made to achieve a one-stop flood management service, using Jakarta as a case study. The proposed methodologies have three values: sensing, understanding, and acting. First, we build sensors to measure various flood parameters in the sensing approach. Second, we collect all data output from the previous system to provide robust analysis in the understanding part. Finally, in the acting module, we provide a dashboard for the decision support system in the flood management system. Although the system has been established, several challenges to achieving a comprehensive flood management system are clarified in this study, especially data management and governance issues. We conclude this study with the future applications of the flood management system that can be expected to minimize the risk of flood disasters in Jakarta[3][12]

Driving behavior analysis has been examined from a fresh angle that fills in the gaps between research on driving behavior that uses simply the GPS signal in uncontrolled tests and those that use CAN bus data in extremely controlled experiments. This paper presents a mechanism for identifying commonalities among drivers based on information gathered in an entirely uncontrolled experiment, by applying a distributional approach to a clustering algorithm that is applied to seven distinct aspects of eight signals recorded by CAN bus sensors. 4.3 Kumar Hemanth and Sentamilselvan K "Customer Contentment with Call Taxi Services" An analysis mentioning Chennai. The organized taxi services sector is highly competitive, thus businesses must use promotions to entice customers. Customers' creative activity encourages the download of mobile apps and others Given that price-conscious shoppers are likely to utilize coupons, the study's findings are in line with previous research studies.[4][13].

A. Tables

TABLE I CLASSIFIED DISASTER

Subgroup I	Climate & water-related disaster	Cloud bursts, heat waves, cyclones, cold waves, droughts
Group II Subgroup II	Geologically related disasters	Dam failures, dam bursts, mine fires.
Subgroup III	Nuclear-related, chemical, Indus disaster.	Industrial, chemical, and nuclear disasters.
Subgroup IV	Accident related disasters	Oil spill, air, road, rail accidents
Subgroup V	Biologically related disaster	Biological disaster & epidemics

IV. EXISTING SYSTEM

Consider a novel kind of technology that acts as a digital superhero to ensure information security and dependability in difficult situations in disaster-affected areas: a decentralized, lightweight blockchain. This innovative approach employs a blockchain to track misbehavior and record data transactions, adding an extra layer of security against potential assaults and guaranteeing that the shared information is safe and irreversible.

To explain it plainly, let me say this. It's essential to communicate and exchange vital information during disasters. However, there is a chance of malicious attacks or efforts to change the shared data. An answer to this is provided by a decentralized blockchain, which operates similarly to a

digital ledger. Think of this blockchain as an open-access digital diary for all stakeholders involved in disaster aid. In addition to logging data exchanges, it keeps tabs on any wrongdoing or dubious activity. This diary is distributed across multiple computers instead of being stored in one place, making it decentralized. Decentralization is like sharing copies of your journal with several trustworthy friends who can vouch for the authenticity and validity of the information. This paper examines countermeasures and outlines three sorts of potential cyberattacks that could happen in the contemporary digital environment. It seems like superheroes (defenses) preparing to battle various villains in the city (network) (attacks). These safeguards are necessary to maintain the efficacy and security of data sharing during emergencies. In this sense, the blockchain serves as a superhero's shield. It offers a safe and permanent record, meaning that information that has been recorded cannot be altered or erased by anyone. This ensures the completeness and reliability of the information shared between various nodes, which may include emergency responders or law enforcement. Using blockchain technology is like having a vigilant digital security guard watching over the network all the time to protect shared data from malicious behavior. The atmosphere for disaster management is made safer and more efficient by this intelligent and dependable technology, which enhances data transaction security and monitors any unlawful behavior.

V. TECHNIQUES

The fundamental idea behind the "Lightweight Vehicular Blockchain" concept is to leverage a decentralized, lightweight blockchain system specifically created for automotive situations. With its enhanced security and immutability, blockchain technology offers a solid basis for this innovative technique of tracking malicious activity and recording data transfers within the context of vehicle networks. The term "lightweight" implies that this blockchain is designed to work well in automotive settings with constrained resources, ensuring that the processing requirements for the onboard systems of automobiles are kept under control. The emphasis on decentralization, which implies that the blockchain ledger is distributed over multiple network vehicles as opposed to depending on just one authority, is an important characteristic. However, the purpose of data transaction recording is to securely record the data that is transmitted between automobiles. Among the crucial details on traffic patterns, potential dangers on the road, and coordinated maneuvers could be added. All users of the car network can rely on the recorded data because the blockchain safeguards the integrity and confidentiality of these conversations. Security is essential in vehicle situations where data reliability is necessary for efficient and safe mobility. it encourages secure communication, transparent data capture, and effective tracking of misconduct, and eventually contributes to the development of safer and more intelligent transportation systems.

VI. DISADVANTAGE

- As the network grows, there may be challenges and performance issues that arise, so it becomes crucial to consider how scalable the consensus process and the framework are. The ability of a system to handle a growing number of users or transactions is known as scalability.
- In the context of blockchain technology, scalability of the framework refers to how well it can adapt and maintain performance as the number of users or activity inside the network increases.

- The consensus method, which validates and verifies transactions, must also be scalable to maintain optimal processing rates.
- Ignoring scalability problems may result in general network inefficiencies, bottlenecks, and longer transaction processing times.
- Thus, as networks expand, robust scalability methods become crucial to maintaining the blockchain framework

A. Tables

TABLE I DISASTER PROFILE OF INDIA

year	Affected disaster	details
2000-2001	31 (Rajasthan)	Affected population 330.41 lac;damaged crop 3511.77 crore;cattle 399.69 lac
2001-2002	18 (Rajasthan)	Affected population 69.70 lac;damaged crop 1252.27 crore;cattle 69.73 lac
2002-2003	32 (Rajasthan)	Affected population 447.80 lac; damaged crop 4414 crore.

VII. PROPOSED SYSTEM

Crisis management and evacuation procedures must adopt a more organized, technologically sophisticated approach, and this program seems to be a vital response to that requirement. Having a comprehensive organization that can identify and respond to unexpected disasters, regardless of their cause—human action or other factors—becomes essential. The primary benefit of this framework is its capacity to promptly recognize various types of disasters and facilitate a well-coordinated and efficient response. The Debacle Management Framework aims to change how we react to and handle crises by utilizing technology. Increasing the accuracy and speed with which information is relayed to authorities and rescuers is one of the primary objectives of catastrophe identification. This allows them to arrange evacuation operations more precisely and effectively. As a technical ally, the framework streamlines the sometimes challenging and time-sensitive

disaster response process. Real-time data monitoring, resource allocation, and rescue operation coordination are only a few of its numerous and varied capabilities. Beyond its ability to respond quickly, the Disaster Management Framework is special. With tactics for reducing damage over time, it proposes a holistic approach to disaster management. The approach serves to lessen the overall impact of disasters by enabling data-driven decision-making on a solid basis. Furthermore, it is critical for ensuring human safety and preserving life in disaster-affected areas. This research represents a truly groundbreaking step toward a more adaptable and robust paradigm for catastrophe management. Through the combination of technology, timely information, and a proactive strategy, the Disaster Management Framework is a beacon of hope in the face of adversity, aiming to improve community safety and security and dramatically influence places that are prone to disasters. This research represents a truly groundbreaking step toward a more adaptable and robust paradigm for disaster management. Through the combination of technology, timely information, and a proactive strategy, the Disaster Management Framework is a beacon of hope in the face of adversity, aiming to improve community safety and security and dramatically influence places that are prone to disasters.

VIII. TECHNIQUES

In the domains of database administration and cryptography, SQL procedures, SHA-256 (Secure Hash Algorithm 256-bit), and the Advanced Encryption Standard (AES) algorithm are fundamental components, each serving distinct yet connected purposes. Strong security features are a well-known characteristic of the symmetric encryption technique AES. It operates with fixed-size data blocks and is used to encrypt sensitive data, ensuring confidentiality in communication and storage systems. There is a clear interaction between the AES, SHA-256, and SQL procedures in secure database administration. Before being saved, sensitive data might be encrypted with AES to render it unreadable without the right decryption keys. SHA-256 hashes can be used to generate checksums for stored data, ensuring that the data hasn't been altered and simplifying integrity checks. In conclusion, SHA-256, SQL processes, and the AES algorithm work well together in the domains of cryptography and database administration. AES offers strong data encryption, SHA-256 hashing ensures data integrity, and SQL procedures enable safe and efficient database interactions. These components come together to produce dependable and secure information systems, which are essential for safeguarding private information in a variety of settings and applications.

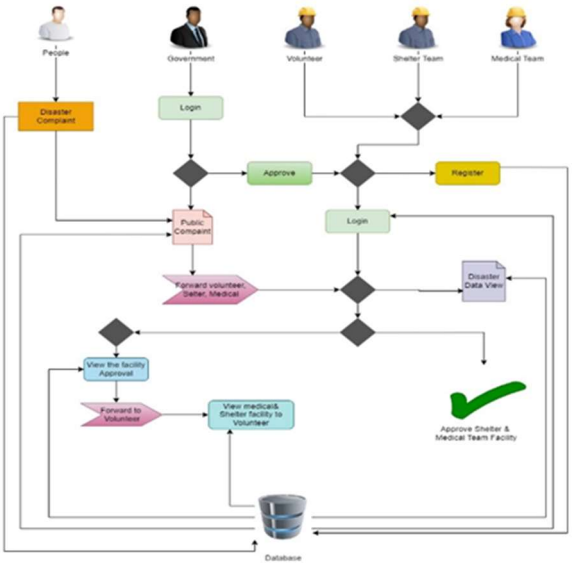

Fig. 1. System Architecture

IX. ADVANTAGE

The popular cryptographic protocols SHA (Secure Hash Algorithm) and AES (Advanced Encryption Standard) are better at hashing and encrypting data than a full blockchain implementation, which requires a lot of resources. AES and other symmetric encryption algorithms are renowned for their quickness and flexibility in safeguarding data while it's being stored or transported. Its ability to process large volumes of data rapidly while maintaining stringent security standards accounts for its efficiency. SHA, and particularly SHA-256, is a hashing technique that ensures data integrity by swiftly producing a fixed-size hash result by generating unique IDs for various inputs.

X. AES ENCRYPTION

Encryption is one of the most basic cybersecurity approaches; it may be used to safeguard sensitive data even if the network it is on has been compromised. In other words, encryption turns plain text into a code that only the owner of the cipher, or key, can decode back into plain text.

A. How Does AES Encryption Work?

The same key or cipher is used by AES, a symmetric block cipher, to both encrypt and decode data. However traditional symmetric encryption is not at all like the AES encryption method. Initially, messages are encrypted in smaller chunks instead of all at once, and further encryption rounds further impede message deciphering. For a 128-bit key (AES-128), ten rounds are needed; for a 192-bit key (AES-192), twelve rounds; and for a 256-bit key, fourteen rounds (AES-256).

B. The AES algorithm consists of four phases in each round:

•Substitution: The algorithm replaces the plain text with the encrypted text based on a predefined cipher.

•Shifting: All the rows are shifted by one, except the first.

•Mixing: Another cipher, called the Hill cipher, is used to mix the columns to prevent someone from merely shifting the rows back to start decrypting the data.

•Further encryption: A small portion of the encryption key is used to encrypt that data block.

XI. AES DESCRIPTION

AES decryption is similar to AES encryption, however it's simpler and essentially the opposite of it.

A. What Is SHA-256?

Safe Hashing Method SHA-256, also known as 256-bit, is a cryptographic hash function that can convert any text into an almost unique 256-bit alphanumeric string. The result is known as a hash or hash value.

B. SHA-256 Explanation: Important characteristics of SHA-256 encryption

The following crucial components enable SHA-256 to fulfill its objectives:

•Uniqueness SHA-256 hash function allows diverse inputs to produce unique hash results every time. Even with a small alteration in the input, a hash value will vary significantly. This is known as the "avalanche effect.".

Irreversibility It is computationally difficult to reverse engineer SHA-256 hash values, hence the original input data for the hash value cannot be extracted.

•Deterministic You may demonstrate the deterministic characteristic of the SHA-256 hash algorithm by verifying the input and output of the previously mentioned "m," "me," and "means you" on several online hash generators, including OnlineWebToolKit and Moveable Type Scripts.

XII. REQUIREMENTS

A. Hardware Requirements

The hardware requirements should be a comprehensive and uniform definition of the entire system since they might form the foundation of a contract for the system's implementation. Software engineers use them as the foundation for their system designs. It illustrates the functionality of the system rather than how it ought to be used.

• PROCESSOR : DUAL-CORE 2 DUOS
• RAM : 2 GB DD RAM
• HARD DISK : 250 GB

B. Software Requirements

The system specification is found in the software requirements paper. It ought to have a description and a list of prerequisites. Rather than focusing on how the system should operate, it is a list of what it should perform. The foundation for developing the software requirements specification is provided by the software requirements. It is helpful for cost estimation, organizing team activities, carrying out tasks, managing teams, and monitoring the teams' advancement during the development process.

• FRONT END : J2EE (JSP, SERVLET)
• BACK END : MY SQL 5.5
• OPERATING SYSTEM: WINDOWS 7
• IDE : ECLIPSE

XIII. FUTURE ENHANCEMENTS

1. generating a workable database structure.

2. improving the efficiency of protocols in terms
of the amount and size of transferred messages.
3. To implement, use two or more algorithms.

XIV. CONCLUSION

The systematic process of managing the impacts of catastrophic events on people, property, finances, and the environment, regardless of whether they are caused by humans or by nature, is known as disaster management. It covers the procedures for preparing, responding, and learning from significant errors. Natural and man-made disasters, including industrial mishaps, earthquakes, and floods, pose serious challenges that necessitate well-thought-out mitigation and recovery strategies. Prompt and well-thought-out evacuation procedures are essential to safeguarding affected people's lives and property during disasters. To address these problems, the proposed framework offers an easy-to-use and productive platform that encourages efficient evacuation procedures and crisis management overall. The "Rescue People" module is crucial in this situation since it enables volunteers and qualified individuals to register and participate in rescue efforts. These individuals assume the role of first responders, providing crucial assistance to victims of disasters and ensuring their prompt evacuation from affected areas. For governmental bodies in charge of disaster management, the "Government" module offers a comprehensive tool. Coordinating rescue efforts, supplying resources for evacuation missions, and real-time data monitoring are all made feasible by this module. The platform guarantees that those in charge may allocate resources to lessen the impact of disasters in a timely and efficient manner. For those who find themselves stranded in disaster-affected areas, there is a module called "Disaster Victims." They now have a simple-to-use mechanism to ask for assistance, receive critical updates, and gather essential information regarding their evacuation thanks to this module. Having a direct channel of communication helps ensure that victims get the help they need as quickly as possible. The administrative portion of the program is managed by the "Admin" module, which provides centralized management over it. Administrators can monitor user accounts and system performance in addition to ensuring the framework functions properly overall. This makes sure that everything goes as planned, which increases the effectiveness of disaster management.

The framework also uses web scraping to incorporate data from outside sources, like websites that provide weather forecasts, in addition to these modules. With the addition of real-time weather data, which is essential for making educated judgments during catastrophic occurrences, the platform's capabilities are improved.

REFERENCES

[1] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Advances in Cryptology — CRYPTO 1992, pages 56–73. Springer, 2004.

[2] [2] Josh Benaloh, Daniel Cohen. elections with a verifiable secret ballot. Yale University, PhD thesis, 1987. [24] Michael J. Fischer and Josh D. Cohen. A strong and independently verified cryptographic election system. Department of Computer Science, Yale University, 1985.

[3] [3] Sako Kazue and Kilian Joe. a mix-type voting system without receipts. Pages 393–403 in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1995.
[4] [4] Electronic voting methods for large-scale elections without receipts, Tatsuaki Okamoto. Pages 25–35 in International Workshop on Security Protocols. Springer, 1997.
[5] [5] Kazue Sako and Martin Hirt. Effective voting without receipts using homomorphic encryption. Pages 539–556, International Conference on the Theory and Applications of Cryptographic Techniques. 2000's Springer.
[6] [6] Adi Shamir and Amos Fiat. Realistic answers to identity and signature issues: How to establish your credibility. Advances in Cryptology — CRYPTO' 86, Berlin, Heidelberg, 1987, pp 186–194. Springer Heidelberg, Berlin.
[7] [7] Zhaoman Liu, Wenlei Qu, Lei Wu, Wei Wang, and Hao Wang. a blockchain-based electronic voting protocol using homomorphic sign cryptography. Practice & Experience with Concurrency and Computation, page e5817, 2020.
[8] [8] "Extracting kernel dataset from huge sensory data in wireless sensor networks," S. Cheng, Z. Cai, J. Li, and H. Gao, IEEE Transactions on Knowledge and Data Engineering, vol. 29, no. 4, pp. 813–827, 2017.
[9] [9] "Drawing dominating dataset from huge sensory data in wireless sensor networks," S. Cheng, Z. Cai, J. Li, and X. Fang, 2015 IEEE Conference on Computer Communications (INFOCOM). 2015 IEEE, pp. 531–539.
[10] [10] "Sinr-based maximum link scheduling with uniform power in wireless sensor networks," B. Huang, J. Yu, D. Yu, and C. Ma, KSII Transactions on Internet & Information Systems, vol. 8, no. 11, pp. 4050–4067, 2014.
[11] [11] "Secure and efficient data transfer protocol for wireless body area networks," C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 2, pp. 94–107, 2016.
[12] [12] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, “Body area network security: a fuzzy attribute-based encryption scheme,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 37–46, 2013.
[13] [13] Opfka: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks, C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2274–2282.
[14] [14A Privacy-preserving communication protocol for Internet of Things applications in smart homes, by T. Song, R. Li, X. Xing, J. Yu, and X. Cheng, will be presented at the 2016 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI).
[15] "Concept of smart home and smartgrids integration," by M. Naglic and A. Souvent, in Energy (IYCE), 4th International Youth Conference, June 2013.