**REVIEW**

|  |  |
| --- | --- |
| Title | **Security in the Internet of Things : A Review** |
| =Type | International Conference on Computer Science and Electronics Engineering |
| Volume & Page | - |
| Year | 2012 |
| Author | Hui Suoa, Jiafu Wana,b  Caifeng Zoua, Jianqi Liua |
| Reviewer | Hendri Purnomo , Asep Irawan, Danang A.M, Tetra Praja.U |
| Date | 25 November 2019 |
| Introduction | * Internet of things is a concept where internet connectivity can exchange information with each other with the objects that are around it * security hole on iot ( munication data, hardware device, web service, aplication) * type of attack on iot (DDOS,  Brute Force Attack, Sql injection etc.) * solution to overcome attacks |
| Objective(s) | The research is to show the status of key technologies including :  encryption mechanism  communication security  protecting sensor data  cryptographic algorithms |
| Conclution | Brief review of the research progress of IoT about the security. By means of deeply analyzing the security architecture and features, the security requirements are given.. |

**REVIEW**

|  |  |
| --- | --- |
| Title | **Vulnerabilities of Fingerprints Authentication Systems and Their Securities** |
| Type | International Journal of Computer Science and Information Security (IJCSIS) |
| Volume & Page | Vol. 16, No. 3 |
| Year | 2018 |
| Author | Tanjarul Islam Mishu  Dr. Md. Mijanur Rahman |
| Reviewer | Hendri Purnomo |
| Date | 06 December 2019 |
| Objective(s) | The objective of the study is to summerize the vulnerabilities of fingerprint authentication system and to highlight the types of securities available agains those challenges. |
| Subject | Types of attacks on fingerprints systemz: Fake Biometric, Replay Attack, Override Feature Extractor, Synthesized Feature Set, Override Matcher, . Template Database Attack, Database-Matcher Channel Attack, Override Final Decision |
| Strength(s) | * This study conveys a prominent analysis on the vulnerabilities of Fingerprint Authentication System of each point of the model and shows the effective security system existing now. This work brings vulnerabilities and securities, compacted together, of fingerprint authentication system. Different types of attack such as fake biometric, replay data, synthesized feature set and template database have been explained about how they occur. * The paper also contains the prevention techniques against the corresponding attacks. * This paper even shows very small attempts taken such as match on card for the security of fingerprint template. |
| Weakness(es) | Though several types of work have been done on the template security, they are not able to satisfy all the requirements such as recoverability, security, privacy, high matching accuracy etc. So, the probable next project is to generate an efficient template security scheme. |