**Mini Project Report on**



**KEY MANAGEMENT SCHEME FOR SECURE COMMUNICATION**



**Submitted in partial fulfilment of the requirement for the award of the degree of**

**BACHELOR OF TECHNOLOGY**

**IN**

**COMPUTER SCIENCE & ENGINEERING**

**Submitted by:**

**Bhairvi Pant**   **2018760**

***Under the Mentorship of***

**(Dr.) Mohammad Wazid**

**Professor**



**Department of Computer Science and Engineering**

**Graphic Era (Deemed to be University)**

**Dehradun, Uttarakhand**

**July-2023**

GEU logo

**CANDIDATE’S DECLARATION**

I hereby certify that the work which is being presented in the project report entitled **“Key Management Scheme for secure communication”** in partial fulfilment of the requirements for the award of the Degree of Bachelor of Technology in Computer Science and Engineeringof the Graphic Era (Deemed to be University), Dehradun shall be carried out by the under the mentorship of **(Dr.) Mohammad Wazid, Professor**, Department of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun.

Bhairvi Pant University Roll no: 2018760

**Table of Contents**

| **Chapter No.** | **Description** | **Page No.** |
| --- | --- | --- |
| Chapter 1 | Introduction | **1-3** |
| Chapter 2 | Literature Survey | **4-6** |
| Chapter 3 | Methodology | **7-8** |
| Chapter 4 | Result and Discussion | **9-10** |
| Chapter 5 | Conclusion and Future Work | **11** |
|  | References | **12** |

**Chapter 1**

**Introduction**

The Internet of Things, often called IoT, is an intricate labyrinth of physical devices (referred to as “Things”). IoT enables and educates a device on the appropriate decisions without human interference. These devices communicate over the internet in coordination with each other to work in synchronisation. The boom in the IoT industry can be observed in many devices and fields such as refrigerators, Air-conditioners, smart-watches, cars, health monitors, baby monitors, agriculture, smart farming, etc. This growth can be attributed to many factors such as decreased cost of storage and memory over cloud servers and a decrease in the cost of manufacturing and maintenance of IoT devices.[1]

The project is dedicated to establishing a secure communication scheme for IoT devices that communicate with each other over the Internet. This communication is not secure most of the time as malicious attackers are continuously looking for an opportunity to cause havoc in society. Thus our communication becomes vulnerable to many attacks such as Man-In-the-Middle-Attack, Replay Attacks, Message modification attacks, Eavesdropping and many more.

Some of these attacks are discussed briefly:

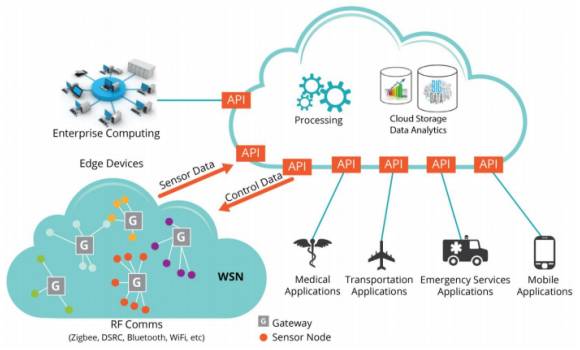
1. Man-In-the-Middle Attack-When two legitimate parties are communicating and a person with malicious intent tries to access, read, and modify those messages we call it a man-in-the-middle attack.

2. Replay Attacks- When a cybercriminal eavesdrops on communication and then either delays or re-transmits a part of that message to misguide the receiving party.

3. Message modification attacks- When messages between legitimate users are modified or tampered with by a malicious person.

4. Eavesdropping - It is also known as sniffing or passive attack where a person with malicious intent intercepts an ongoing communication and monitors private data exchange between the two parties.

These attacks can be dodged if the devices are trained to communicate using a secure key management scheme. This scheme should be able to compute secure keys for the device registration, generation and distribution for all IoT devices.[2]



Traditionally any data exchange could be protected using a single key but when working with such intricate data communication we cannot rely on a single key as the compromise of that one key alone can compromise the security of the entire communication system. Hence we need real-time authentication and protection which can be time-taking and complex.

Some remarkable efforts are seen in the authentication and protection of data transfer in IoT devices with stress on key management including group key management technique (GKMP), mutual key management technique (KMP), Elliptic Curve Cryptography (ECC)/Elliptic Curve Diffie Hellman (ECDH) based key management etc. Either symmetric and Asymmetric cryptography systems are used in each of them.

**Chapter 2**

**Literature Survey**

1. Ntshabele, K., Isong, B., and Gasela [3] developed a security key management server using LoRaWAN(Low Range Wide Area Network) using a cryptographic system similar to AES(Advanced Encryption System)- 128 bits to secure data in transmission. The security verification tool Scyther has been used to verify the strength of the security protocol against various attacks. Two algorithms A and B are designed for a trusted Key Management Server (TKMS). It is important to note that the algorithm B is just a modification or an enhanced version of A as when algorithm A goes under verification in Scyther if the model is unable to protect against attacks it goes under an improvement phase where it is again tested and once it runs successfully it is named Algorithm B. It is also important to note that the authors use an XOR function algorithm to compute the Keys.

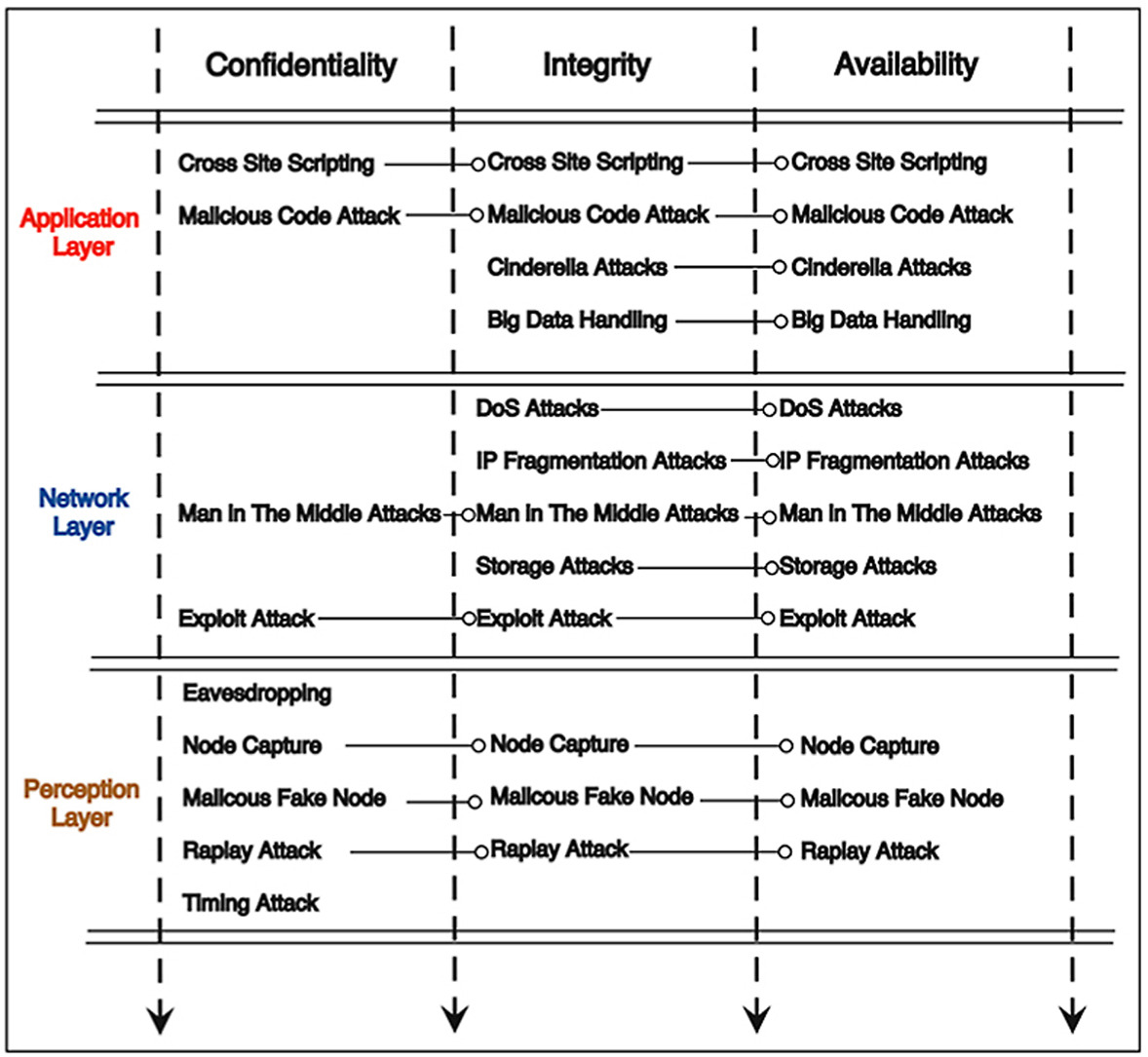
Result: After 7 rounds of improvement algorithm A finally becomes algorithm B and is finally secure.

1. M. Wazid, M. S. Obaidat, A. K. Das and P. Vijayakumar developed a SAC-FIIoT

which is a secure access control scheme for the Fog-Based Industrial Internet of Things. IIoT refers to an industry-level connection of various devices over the internet that communicate with cloud servers as well as each other to exchange information. To design a security model for IIoT they have used Fog-based architecture where devices such as temperature-sensing devices, machines, and gas-measuring devices act as the end devices. The device layers are connected to an intermediate fog layer that is present between the end devices and the main cloud servers. The main concept behind having a fog layer is that the data that is more frequently used can be stored in the fog layers whereas the data less frequently used is stored in the cloud layers. The data stored in these fog layers is also vulnerable to attacks and hence a security protocol is needed. The authors use the “Dolev Yao” threat model is used to design this protocol.

Result: Comparative analysis of this new model proves to be more efficient than the existing models.

1. D. Dragomir, L. Gheorghe, S. Costea and A. Radovici have done a comparative analysis of the different security protocols and networking stacks for IoT that have been designed in recent years. They focus on schemes specified by reputed standardization bodies such as IETF and IEEE, and industry alliances, such as ZigBee Alliance, NFC Forum, LoRa Alliance and Thread Group.
2. Apostolos Gerodimos, Leandros Maglaras, and Mohamed Amine Ferrag[6] have done a comparative understanding and analysis of the three main layers in an IoT framework that are: The Application layer, The Network layer and the Perception Layer. It also discusses about the various attacks that can infiltrate these layers and their security mechanisms. The review of this paper gives us a detailed idea of all the potential attacks that can happen in our IoT framework.

****

1. A. Piccoli, M. -O. Pahl and L. Wüstrich discuss a variation in the point-to-point communication i.e. the Group key management scheme which is one of the popular key management and distribution schemes in IoT devices. This paper studies and surveys existing GKM mechanisms and analyzes their appropriateness for constrained IoT settings, and identifies open problems that require more research.

**Chapter 3**

**Methodology**

The key management scheme of secure communication between IoT devices is written in Security Policy Definition Language(SPDL) and its strength against various attacks can be verified using an automated security verification tool such as Scyther, Tamarin etc. For the scope of this paper, we specifically make use of the Scyther tool. In an IoT framework following are the steps for communication.:

1. Registration of devices in the cloud server
2. User login - 2- factor/3- factor authentication
3. Authentication and session key establishment
4. AI-based data analysis
5. Secure data delivery to Authorized users

In the registration phase the following parameters are calculated:

1. The TA(Trusted Authority is assumed to be an unbiased authority) performs the registration of various entities. The TA and the devices have their secret key and unique identification nTA, idTA and nDiv, idDiv. The TA computes the puedo-identity(RID) of the device using the hash-value of (idDiv || nDiv) and similarly its pseudo-identity. After which the TA computes the temporal credential using the hash value of idDiv, RID(TA), nDiv, and RTS(Div) where RTS is the unique time-stamp of the device. It also generated the random temporary identity of the device called TID(Div). The TA finally stores the TID(Div), RID(Div), TC(Div), and the hash of them in the memory of Div.
2. Registration of cloud server: The TA does the registration of each cloud server CS. It chooses the identity of the cloud server as ID(CSj) and then computes the pseudo-identity of CSj as TC(CSj). The TA finally stores this in the memory of CSj before its deployment in the cloud server.

This marks the end of the registration phase for the devices and the cloud servers.

1. Authentication and Key establishment phase: This phase is required for the secure authentication of the devices and the cloud servers. idDiv is the initiator therefore it generates a random nonce rs1 and t1. It then computes M1 and M2 as the hash function and then Div sends an authentication message Msg1 as the concatenation of M1, M2, and T1 to CSj. After receiving the Msg1 the CSj verifies the timeliness of the message using “Maximum Transmission delay”. If it matches the Msg’1 calculated by CSj the CSj generates rs2 and T2 and computes M3 as a hash function.

Now the session key in the cloud is generated and using this session key M4 is generated as hash value, a new temporary id of Dvi and a new message M5 as hash value. Using the XOR of all these values msg2 is calculated.

1. After receiving msg2 from CSj, Div now verifies the timeline T2 using maximum transmission delay. The session key is now generated by Div and using this session key M4 is generated. Parallelly M4’ is calculated by Div. If they match then CSj is authenticated with Div.
2. Div generates time-stamp T3 and computes a session key verifier skv. After receiving Msg3 from CSj, Div verifies the timeline of T3 using “maximum transmission delay” and computes skv’. If skv==skv’ then the session key computed by Div is correct and a secure data transmission is established between CSj and Div.
3. This step marks the end of the Authentication and verification step by CSj and Div and ensures the secure transmission of data.

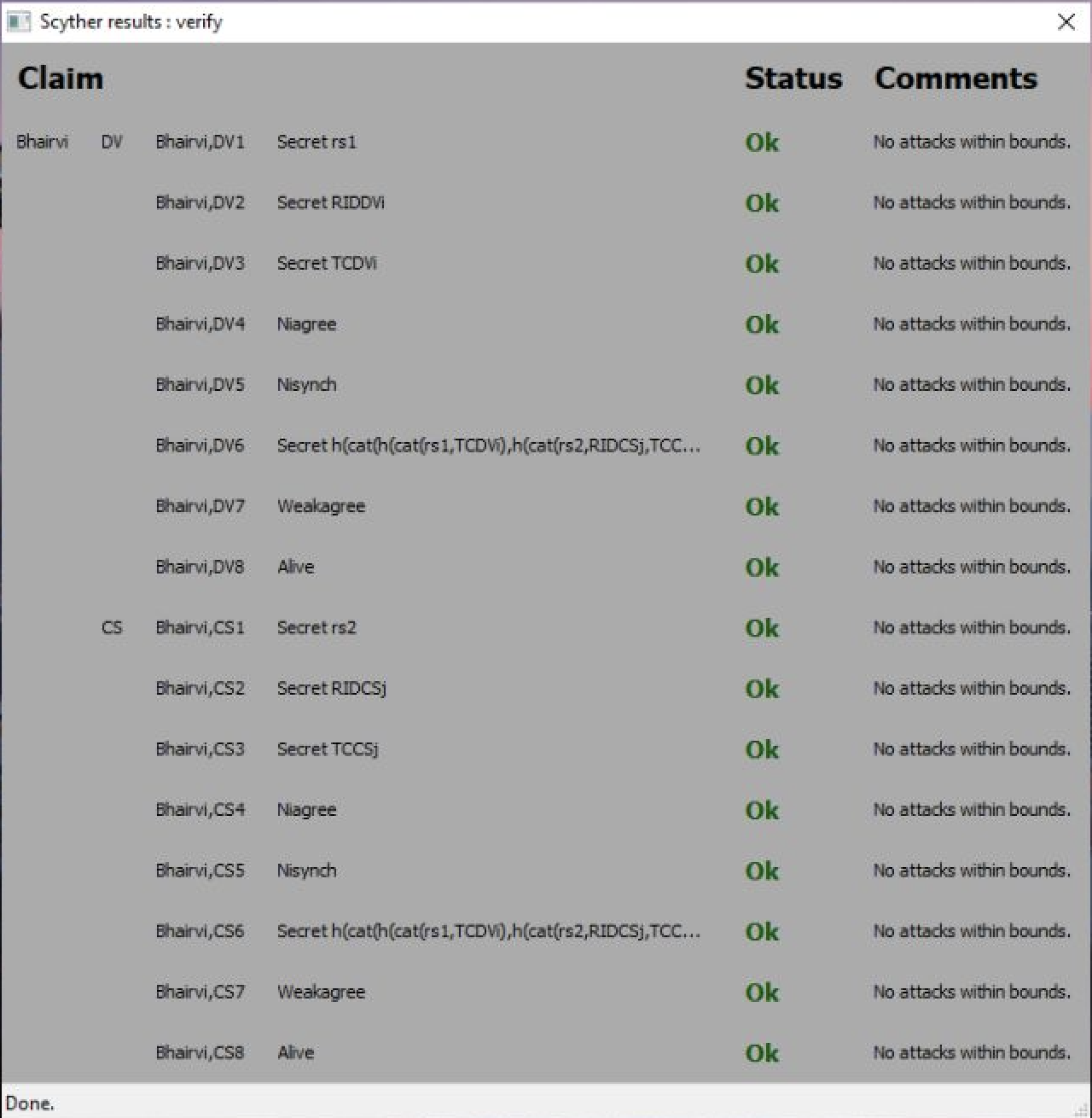
The following protocol written in SPDL can be run in Scyther and tested against many attacks.

The proposed framework relies mostly on XOR, concatenation and Hash function which make sure that even a slight modification in the parameters of the hash function or the XOR can change the output drastically. This effect is called the “Avalanche Effect” and contributes majorly to the confidentiality and Integrity of our messages.

**Chapter 4**

**Result and Discussion**

Upon writing this protocol in SPDL and testing this transmission scheme on the automated security verification tool Scyther we see that it is secure from every attack possible on the IoT device. We can see the report analysis and performance of this scheme through the following diagram:

****

We can see that it performs positively on all parameters.

**Chapter 5**

**Conclusion and Future Work**

Through the above discussion and the proposed framework, we can conclude that our proposed mechanism is secure against all given types of attacks and can be improved more by training and testing it against more attacks. The use of hash functions almost at every step of computations ensures that even a slight change in the parameters will drastically affect the computed value. In future, we can add more solid parameters that improve the security of our protocol. We can even interchange the parameters making it more robust.

**References**

[1] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, K. -K. R. Choo and Y. Park, "On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System," in IEEE Transactions on Vehicular Technology, vol. 70, no. 2, pp. 1736-1751, Feb. 2021, doi: 10.1109/TVT.2021.3050614.

[2] Tabassum T, Hossain SKA, Rahman MA, Alhamid MF, Hossain MA. An Efficient Key Management Technique for the Internet of Things. Sensors (Basel). 2020 Apr 6;20(7):2049. doi: 10.3390/s20072049. PMID: 32268487; PMCID: PMC7181291.

[3] Ntshabele, K., Isong, B., Gasela, N., & M., A. (2022). A Trusted Security Key Management Server in LoRaWAN: Modelling and Analysis. *Journal of Sensor and Actuator Networks*, *11*(3), 52. <https://doi.org/10.3390/jsan11030052>

[4]M. Wazid, M. S. Obaidat, A. K. Das and P. Vijayakumar, "SAC-FIIoT: Secure Access Control Scheme for Fog-Based Industrial Internet of Things," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9322212.

[5] D. Dragomir, L. Gheorghe, S. Costea and A. Radovici, "A Survey on Secure Communication Protocols for IoT Systems," 2016 International Workshop on Secure Internet of Things (SIoT), Heraklion, Greece, 2016, pp. 47-62, doi: 10.1109/SIoT.2016.012.

[6] Apostolos Gerodimos, Leandros Maglaras, Mohamed Amine Ferrag, Nick Ayres, Ioanna Kantzavelou, IoT: Communication protocols and security threats, Internet of Things and Cyber-Physical Systems, (https://www.sciencedirect.com/science/article/pii/S2667345222000293)

[7] A. Piccoli, M. -O. Pahl and L. Wüstrich, "Group Key Management in constrained IoT Settings," 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 2020, pp. 1-6, doi: 10.1109/ISCC50000.2020.9219619.