Comparison of encryption algorithms for wearable devices in IoT systems

Hao Zhou

Abstract

The thesis is about the comparison of encryption algorithms for wearable devices. Because the most popular wearable devices in the market are smart watches,choosing the smart watches as sample to analysis. Moreover, based on the current cryptographic protocol standards that are being used in IoT, choosing AES, PRESENT,RSA and ECC algorithms as the comparison in the encryption algorithms. Also, the hybrid algorithm called HAN show impressive potential and security in encryption.

1 Introduction

The Internet of Things (IoT) is composed of many devices that are connected through the Internet.[8] IoT devices has become highly popular and has penetrated new markets as well which can help humans to upgrade their daily lifestyle.[7] The common IoT devices in the market are smart watches, smart glasses, smart shoes and so on. Wearable devices collect sensing information, and transfer sensing information from user to servers via the Internet. Wearable devices, users and server communicate over a public (insecure) channel as they are connected through the Internet[8] or Bluetooth. Because the sensing information includes human activities, heart rates, daily route, and the environmental information, it's essential to ensure smart devices has strong security and encryption algorithms. On the other hand, compared with smart Phone and computer, wearable devices have a smaller size and higher demand for the energy control. Wearable devices cannot directly replicate the encryption strategy from the smartphones and computers. Current cryptographic protocol standards that are being used to provide security for wearable devices include Secure Hash Algorithm (SHA), Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman(RSA).[8]

1.1 Security attacks for wearable devices

Communications in wearable devices happen via Internet or Bluetooth, which is a publically available network. This makes it susceptible to various attacks which cause interruption in smooth working of wearable devices. Some serious security vulnerabilities may lead to theft of user data and the spread of viruses.[2]Some attacks are discussed below.

- **Eavesdropping**: This attack is on the confidentiality as the intruder gets hold of the data being shared between sender and receiver. The other devices can constantly monitor data of the compromised device and can also transmit false messages to gather personal data of that device.[30]

- **Denial of Service Attack**: This attack stops the services of the network for authorized users as unauthorized users try to connect to that network. DOS in Physical Layer causes Jamming (the channel used for communication between the nodes is occupied by unauthorized party), node tampering (sensitive information is extracted by physical tampering of the nodes). On network layer DOS attack causes spoofing (a useless message is sent by a malicious node which is then replayed by the attacker to generate a high traffic).[21]

- **Man-in-Middle**: In this attack an intermediary user gets the key of one of the communicating party and starts exchanging information as if it is the valid party. It is a dangerous attack, the attacker fakes as the original sender. The attacker can trick the recipient into thinking they are still getting a correct message.[6]

- **WiFi hacking**: This is essentially cracking the security protocols in a wireless network, granting full access for the hacker to view, store, download, or abuse the wireless network. Usually, when someone hacks into a WiFi, they are able to observe all the data that is being sent via the network.

- **Wormhole**: This DoS attack causes rearrangement of bits of data from its original position in the network. An attacker records bits at one location in the network, channels them accordingly to another location, and then retransmits them there into the network.[11]

- **Fabrication**: The attacker causes unauthorized insertion, modification of data into the IoT system. This causes threat to the authentication of the system as the sender has no knowledge that the system is compromised.[16]

1.2 Security analysis on real examples of wearable devices

The most popular wearable devices in the market are smart watches and smart glasses. The main player in wearable devices are Apple, Samsung, XiaoMi and Google.

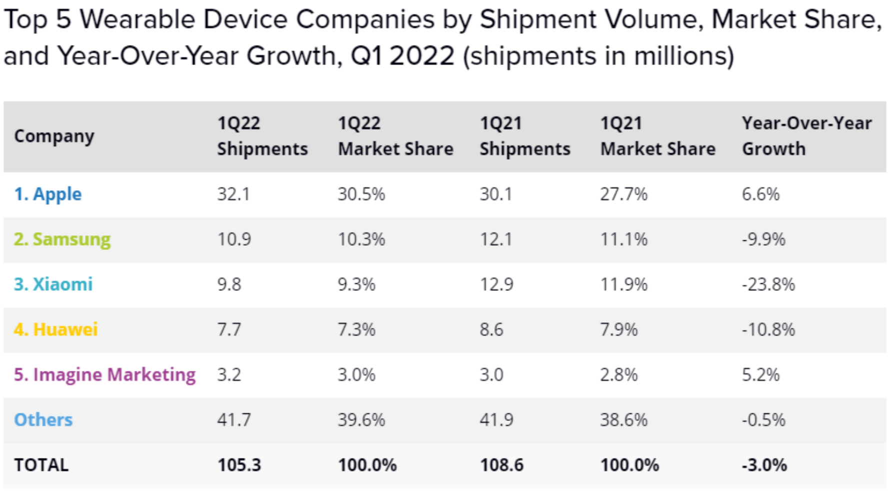
- **Apple Watch**:is a smartwatch developed by Apple Inc. It incorporates fitness tracking, health-oriented capabilities, and wireless telecommunication, and integrates with iOS and other Apple products and services. The Apple network communication primarily in conjunction with the user's iPhone, but can separately connect to a WiFi network for some data-reliant purposes.

- **Samsung watch**: is a smartwatch developed by Samsung Electronics in 2018. It also incorporates fitness tracking, health-oriented capabilities, and wireless telecommunication, and integrates with Samsung smart phone or Android smartphone.

- **XiaoMi watch**: is a smart band developed by XiaoMi in 2014. It also incorporates fitness tracking, health-oriented capabilities,and integrates with XiaoMi smart phone or Android smartphone.

- **Google glasses**: is a brand of smart glasses developed by Google in 2013. It was the first impression-level smart wearable device, and its emergence has led to the stimulation and development of the wearable devices market.

Hence, choosing Apple watch, Samsung watch, XiaoMi watch, Google glasses as the real example to analysis.



Top 5 Wearable Device Companies by Shipment Volume, Market Share, and Year-Over-Year Growth, Q1 2022 (shipments in millions)

Company	1Q22 Shipments	1Q22 Market Share	1Q21 Shipments	1Q21 Market Share	Year-Over-Year Growth
1. Apple	32.1	30.5%	30.1	27.7%	6.6%
2. Samsung	10.9	10.3%	12.1	11.1%	-9.9%
3. Xiaomi	9.8	9.3%	12.9	11.9%	-23.8%
4. Huawei	7.7	7.3%	8.6	7.9%	-10.8%
5. Imagine Marketing	3.2	3.0%	3.0	2.8%	5.2%
Others	41.7	39.6%	41.9	38.6%	-0.5%
TOTAL	**105.3**	**100.0%**	**108.6**	**100.0%**	**-3.0%**

Figure 1: Wearable Devices Market Share

Table 1: Summary of Security Vulnerabilities and Attacks in Wearable Devices

Wearable Devices	Security Vulnerabilities	Attacks
Apple Watch	A validation issue was found. A malicious application may be able to gain root privileges.[24]	Fabrication: The attacker causes unauthorized insertion, modification of data into the system
Apple Watch	A certificate parsing issue. A malicious app may be able to bypass signature validation.[27]	Fabrication: The attacker causes unauthorized insertion, modification of data into the system
Apple Watch	Out-of-bounds access issue, A malicious application may be able to execute arbitrary code with system privileges.[26]	Fabrication: The attacker causes unauthorized insertion, modification of data into the system
Apple Watch	GasGauge in Apple watchOS allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	Denial of Service Attack(DOS)
Samsung Watch	The authentication mechanism was not strong and secure enough.[10][19]	Brute Force
Samsung Watch	Information Exposure vulnerability in Galaxy S3 allows attacker with log permissions to leak Wi-Fi password connected to the user smartphone within log.[25]	Wifi Hacking
XiaoMi Band	Some js interfaces in the Xiaomi community were exposed, causing sensitive functions to be maliciously called.[23]	Man-in-Middle and Eavesdropping.
XiaoMi Band	Unsecure Bluetooth communication [17] and internet communication.	Man-in-Middle and Eavesdropping.
XiaoMi Band	Unsecure authorization [17]	Fabrication: The attacker causes unauthorized insertion, modification of data into the system
Google Glass	Unsecure PIN system or authentication in place.[9]	The gesture-based authentication scheme easily to be recorded by people nearby.
Google Glass	Unsecure network and hostile environment.[28]	Wi-Fi-hijacking, man-in-the-middle attacks such as session hijacking or sniffing
Google Glass	Pictures and video can be recorded without user's consent and unauthorized eye movement tracking[20]	Eavesdropping and spyware

The table above shows that there are many common security vulnerabilities inside the wearable devices. Some attacks such as Dos, Fabrication, Eavesdropping and spyware can cause significant damage to user privacy and security of user devices. If these attacks reach the user's device, it will cause the user's personal information to be stolen, the user will not be able to use the device properly and the user will receive tampered and fraudulent messages. Some of the vulnerabilities have been improved. However, it showed that current security precautions are still not adequate. It still has a lot of improvements that can be made.

1.3 Security challenges for wearable devices

The attacks on IoT network is discussed so to keep all connected devices secure security required. The IoT security classify in 3 ways. These are security and data protection, authentication and identity management, and Privacy.

- **Security and Data Protection**: Since wearable devices are wireless and share sensitive information on public networks.They become vulnerable to malicious attacks and information theft, so it requires advanced technologies to secure the system. [29]Cryptographic algorithms are a good way to secure the information security of wearable devices. Because of wearable devices features, cryptographic algorithms need less energy consumption,but should not compromise on their efficiency.[1]

- **Authentication and Identity management**: It is an important component of any security model. Each object in the IoT network should be able to identify and authenticate other objects. A unique identifier can be used to create a personal identity for these objects. The personal identity of these objects. It ensures the identity of smart objects before any communication between them.A mechanism that enables devices to authenticate with each other before each interaction before each interaction is very crucial for the success of the IoT.[13]

- **Privacy**:As objects become traceable through the Internet of Things, privacy-related threats have increased exponentially. It is important to ensure that data is secure so that it cannot be misused by any third party. Nevertheless, issues related to data ownership should also be addressed. In order to make users feel comfortable in being part of an IoT system, measures must be taken. The ownership of the information collected from different smart objects must be clearly established. Owners must be assured that their data will not be used without their consent, especially when the data is shared on the Internet.[12] The privacy of the information can be ensured through privacy policies. Smart devices can be equipped with these policies. Thus, when smart objects come in contact with each other, they can be compatible through their respective privacy policies before exchanging any information.[18]

2 Encryption algorithms for wearable devices

Overview of Cryptography for Wearable devices: Cryptography is a technique in which we can encrypt data into cipher text for its secure transmission. Cryptographic ciphers are of two types, symmetric and asymmetric ciphers. Symmetric key encryption uses same key for both encryption and decryption of data. This method of encryption is extremely secure and relatively fast.[3]Some of the symmetric key ciphers are AES(Advanced Encryption Standard) and PRESENT. In addition, Asymmetric key encryption uses two keys, private and public key for communication between the sender and receiver. Asymmetric encryption provides authentication, confidentiality and integrity. To ensure confidentiality and Integrity the sender uses public key for encryption of data and the receiver uses his private key to decrypt it.[3]Some of the asymmetric encryption are RSA(Rivest–Shamir–Adleman) and ECC(Elliptic-curve cryptography).

2.1 Introduction of lightweight encryption algorithms for wearable devices

Symmetric Encryption

- **AES**: Advanced Encryption Standard is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is widely adopted and supported in both hardware and software. AES has built-in flexibility of key length, which allows a degree of ‘future-proofing’ against progress in the ability to perform exhaustive key searches. It is a symmetric block cipher, works on the block length of 128 bits with variable key sizes of 128, 192, 256 bits. It is based on substitution permutation network (SPN).
- **PRESENT**: is also based on SPN structure. It is one of the ultra-lightweight algorithms used for security. It has key size of 80 or 128 bits and operates on blocks of 64-bit.[4]PRESENT aims to provide the equally security under extremely constrained environments such as RFID tags and sensor networks.

Table 2: Security and performance analysis between AES and PRESENT

Ref.	Algorithm	Block Size	Structure	Performance				Analysis
				Tech(uM)	Power(uW)	Area(GE)	Throughput(kbps)	
[15]	AES	128	SPN	0.13	2.48	2400	56.64	Supports larger key size, faster in both hardware and software.
[5]	PRESENT	128	SPN	0.18	2.00	1339	12.12	Ultra Lightweight cipher, Energy efficient

Asymmetric Encryption

- **RSA**:Rivest–Shamir–Adleman is a public-key crypto system that is widely used for secure data transmission.An RSA user creates and publishes a public key based on two large prime numbers,along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

- **ECC**:Elliptic-curve cryptography is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security. It has less key size when compared to RSA algorithm. It has less memory requirements and increased computation speed. ECC has proved to be stronger against various attacks in wireless sensor networks and many other wireless suitable environments. It provides the same level of security in a 160-bit key size when compared to security provided by 2048-bit key size of RSA[14][22]

Table 3: Lightweight Asymmetric Algorithm Performance analysis

Ref.	Algorithm	Key Size	Key Generation(s)	Signature Generation(s)	Verification	Analysis
[14][22]	RSA	1024	0.16	0.01	0.01	Increased Security
		15360	679.06	9.20	0.03	
[14][22]	ECC	163	0.08	0.15	0.23	Increased speed, less memory requirement
		571	1.44	3.07	4.53	

The Table shows ECC has better performance and provide high security than RSA when large key size is used. So, in the modern era for authentication purposes ECC will be preferred over RSA in wearable device.

However, in addition to the above four encryption algorithms, there is another algorithm named HAN. As a hybrid algorithm, HAN algorithm is not only fast in processing and generating signature, but also has high security. I will introduce it in the next chapter.

2.2 HAN Algorithms Analysis

Hybrid encryption technique is a new model that can be used in wearable devices. Hybrid encryption technique is for information integrity, confidentiality, being non-repudiation in data exchange for wearable devices.[31]

HAN Creating Key

Key production process in AES is used to create a key. This step of HAN algorithm has been drawn from AEC algorithm. It should be noted that produced key of h is on the basis of hexadecimal. Then public key h is produced. The aim is sending a hidden message from sender to receiver in which private key is just recognized by the receiver and public key by both sender and receiver. So encryption process must have a tight security. It means that the encrypted message by the sender will be sent to the receiver in secret and safety. Therefore NTRU asymmetric encryption is used to enhance the security. When the sent message by the sender is encrypted, it should not be identifiable by any person other than intended recipient. [31]

HAN Encryption

$$Encryption = pr * h + message \tag{1}$$

HAN Decryption

$$a = f * encryption \tag{2}$$

$$a = f * (pr * h + message) \tag{3}$$

$$Because(pr * h = 0) \tag{4}$$

$$Hence(a = b = f * message) \tag{5}$$

$$Decryption = (fp * b)/x^2 \tag{6}$$

HAN Digital Signature

$$Encryptionsign = (message * f)/x^2 \tag{7}$$

$$Decryption = (h/2 * fp * Encryptionsign)/2 * h \tag{8}$$

2.3 HAN algorithm Evaluation

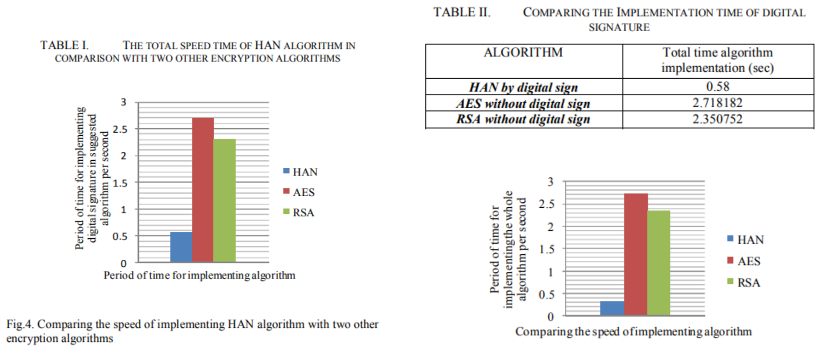


TABLE I. THE TOTAL SPEED TIME OF HAN ALGORITHM IN COMPARISON WITH TWO OTHER ENCRYPTION ALGORITHMS

Fig.4. Comparing the speed of implementing HAN algorithm with two other encryption algorithms

(a) Implementation time evaluation

TABLE II. COMPARING THE IMPLEMENTATION TIME OF DIGITAL SIGNATURE

ALGORITHM	Total time algorithm implementation (sec)
HAN by digital sign	0.58
AES without digital sign	2.718182
RSA without digital sign	2.350752

Period of time for implementingthe whole algorithm per second
3
2.5
2
1.5
1
0.5
0
Comparing the speed of implementing algorithm
HAN
AES
RSA

(b) Implementation time of digitSignature

Figure 2: HAN algorithm Evaluation

The results are shown the speed of the HAN algorithm even with digital signature is less than AES and RSA algorithms. And the total speed time of HAN algorithm is also faster than AES and RSA.[31]

In addition,the percentage of power usage in HAN algorithm is 11/81% of the AES algorithm, and is 13/65% of the RSA algorithm. [31]

2.4 Conclusion of HAN algorithm

HAN algorithm is considered as a suggested method that is a combination of AES symmetric encryption algorithm and NTRU asymmetric encryption algorithm for IOT improvement. This algorithm has high speed to create a key, encryption and decryption and acceptable security in IOT. Safety of this algorithm is because of multinomial usage in encryption, decryption and digital signature to achieve a correct message. This algorithm uses less memory because of less fiscal complexity. This algorithm makes available the encryption in IOT with deduced attacks and improved security.[31]

3 Conclusion

In summary, this thesis explores a overview that is about the Security analysis of the wearable devices and some challenges of the wearable devices.And the overview of encryption algorithms for wearable devices, and the hybrid encryption algorithms called HAN.

References

[1] Debasis Bandyopadhyay and Jaydip Sen. Internet of things: Applications and challenges in technology and standardization. *CoRR*, abs/1105.1693, 2011.

[2] Isha Bhardwaj, Ajay Kumar, and Manu Bansal. A review on lightweight cryptography algorithms for data security and authentication in iots. In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, pages 504–509, 2017.

[3] Isha Bhardwaj, Ajay Kumar, and Manu Bansal. A review on lightweight cryptography algorithms for data security and authentication in iots. 10 2017.

[4] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe. Present: An ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, pages 450–466, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[5] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe. Present: An ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, pages 450–466, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[6] Zoran Cekerevac, Zdenek Dvorak, L. Prigoda, and Petar Čekerevac. Internet of things and the man-in-the-middle attacks – security and economic risks. *MEST Journal*, 5:15–5, 07 2017.

[7] Conurets. Top 10 wearable iot devices in 2022, 2022.

[8] Ashok Kumar Das, Sherali Zeadally, and Debiao He. Taxonomy and analysis of security protocols for internet of things. *Future Generation Computer Systems*, 89:110–125, 2018.

[9] Daniel Dimov. Privacy implications of google glass, 2013.

[10] HP. Hp study reveals smartwatches vulnerable to attack., 2015.

[11] Yih-Chun Hu, A. Perrig, and D.B. Johnson. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):370–380, 2006.

[12] Kai KANG, Zhi bo PANG, and Cong WANG. Security and privacy mechanism for health internet of things. *The Journal of China Universities of Posts and Telecommunications*, 20:64–68, 2013.

[13] Parikshit Mahalle, Sachin Babar, Neeli R. Prasad, and Ramjee Prasad. Identity management framework towards internet of things (iot): Roadmap and key challenges. In Natarajan Meghanathan, Selma Boumerdassi, Nabendu Chaki, and Dhinaharan Nagamalai, editors, *Recent Trends in Network Security and Applications*, pages 430–439, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[14] Dindayal Mahto, Danish Khan, and DILIP YADAV. Security analysis of elliptic curve cryptography and rsa. 06 2016.

[15] Amir Moradi, Axel Poschmann, San Ling, Christof Paar, and Huaxiong Wang. Pushing the limits: A very compact and a threshold implementation of aes. In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, pages 69–88, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[16] Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. Internet of things (iot): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, pages 321–326, 2016.

[17] Yogesh Ojha. Hacked miband 3, 2018.

[18] R.C. Prof and Ramesh Shahabadkar. A comprehensive survey on exiting solution approaches towards security and privacy requirements of iot. *International Journal of Electrical and Computer Engineering*, 8:2319–2326, 08 2018.

[19] Bitdefender Research. Bitdefender research exposes security risks of android wearable devices., 2014.

[20] Seyedmostafa Safavi and Zarina Shukur. Improving google glass security and privacy by changing the physical and software structure. *Life Sciences*, 11, 05 2014.

[21] Amad Shah, Masood Habib, Taimur Sajjad, Muhammad Umar, and Muhammad Babar. Applications and challenges faced by internet of things - a survey. In *Applications and Challenges Faced by Internet of Things - A Survey*, pages 182–188, 01 2017.

[22] Rounak Sinha, Hemant Kumar Srivastava, and Sumit Kumar Gupta. Performance based comparison study of rsa and elliptic curve cryptography. 2013.

[23] CVE vulnerability database. Vulnerability details : Cve-2020-14130, 2020.

[24] CVE vulnerability database. Vulnerability details : Cve-2021-1813, 2021.

[25] CVE vulnerability database. Vulnerability details : Cve-2022-25830, 2022.

[26] CVE vulnerability database. Vulnerability details : Cve-2022-26763, 2022.

[27] CVE vulnerability database. Vulnerability details : Cve-2022-26766, 2022.

[28] Candid W. Google glass still vulnerable to wifi hijacking despite qr photobombing patch, 2013.

[29] Andrew Whitmore, Anurag Agarwal, and Li Xu. The internet of things—a survey of topics and trends. *Information Systems Frontiers*, 17, 04 2014.

[30] Qinghan Xiao, Thomas Gibbons, and Lebrun. *RFID Technology, Security Vulnerabilities, and Countermeasures*, pages 357–382. book, 01 2009.

[31] Afsoon Yousefi and Seyed Mahdi Jameii. Improving the security of internet of things using encryption algorithms. In *2017 International Conference on IoT and Application (ICIOT)*, pages 1–5, 2017.