ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Distributed Secure Data Sharing and Security Issue

Akshitha G N[1], Hemavathi M U[2], Dr. K. S Jagadeesh Gowda[3], Prof. Vanitha T N[4]

B.E Student, Dept of Computer Science and Engineering, Sri Krishna Institute of Technology, Bangalore, Karnataka, India[1,2]

Professor and Head, Dept of Computer Science and Engineering, Sri Krishna Institute of Technology, Bangalore, Karnataka, India[3]

Assistant Professor, Dept of Computer Science and Engineering, Sri Krishna Institute of Technology, Bangalore, Karnataka, India[4]

ABSTRACT: Internet of Things (IoT)has the ability to identify and connect physical objects worldwide into a unified system. IoT is basically combination of both hardware and software. It is the network of physical devices, vehicles, home appliances, and software, sensors, which enables these objects to connect and exchange data.The Information Centric Networking (ICN) paradigm is attracting more and more interest from the research community due to its peculiarities that make it one of the best candidates for constructing the Future Internet. [4]IoT is developing day by day and as it continues to develop,more potential is estimated by combination with related technology concepts such as Cloud Computing,Big Data,Robotics,etc,.IoT is also sometimes called as Internet of Objects(IoO). As a part of IoTs,concerns are raised over access of personal information related to device and individual privacy and even security. In Information Centric Internet of Things (ICIoT),IoT data can be cached throughout the network, but this distributed data caching environment poses authorization challenge.Hence to overcome this problem Cipher text Policy Attribute Based Encryption(CPABE) scheme is identified as the best approach.

KEYWORDS: ICIoT, ICN, IoT

I. INTRODUCTION

Fig.1 Architecture of Internet of Things

Internet is a global communication infrastructure that hosts billion of devices and enables the exchange of Exabytes of data per year.According to its design,the communication is between the data consumer and the data producer.This exchange of data mechanism is considered as host centric in nature:any information is strictly related to the location of nodes that make them available to the field of research,Information Centric Networking(ICN) has emerged as a revolutionary formulation.ICN communication is centric to information or the data rather than the host locations where

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

the information consumers are interested on the information rather than the location of the source.[6]It has many roles that:)each content is addressed through a name that does not containanymorereference to its location;2)the user sends the request of the needed data;3)the request is processed by the network based on the name resolution. Information oriented future internet architectures are Content centric networking(CCN),and Named Data Networking(NDN).The approach of these architectures are commonly called as Information Centric Networking(ICN).NDN is an ICN architecture designed to replace the host oriented communication model in TCP/IP with the data centric one. With the fast growing development of Internet technology and communication, our lives are leading to a imaginary space of virtual world. Any number of people can communicate using network. A new technology is needed to integrate the imaginary and real world on the same platform called as IoTs. It is predicted that over 50 billion devices can be connected in the coming years. Nowadays most of the IoT services are designed based on the internet technology that was conceived for end to end communications. Internet of Things data sharing applications have been developed on the basis of centralized server/clouds that produce redundant and duplicate traffic. This redundant traffic hinders data flow.

II. LITERATURE SURVEY

With reference to [1], Overview of Internet of Things (IoT) with emphasis on enabling technologies, protocols, and application issues. The IoT is enabled by the latest developments in RFID, smart sensors, communication technologies , and Internet protocols. Finally we present details services use-cases to illustrate how the different protocols present in the paper fit together to deliver desired IoTservices.with reference to[2],Converging technologies for smart Environment and integrated Ecosystem Dr.OvidivVermesan, boost the economy while improving our citizens. To achieve these promising results,I think it is vital to enhance users trust in the Internet of Things. With reference to [3], Worldwide dozens of project to redesign the Internet are in progress under the banner of the so-called future Internet research. Some proposals argue that the most important things is to design to accommodate information exchanging. We propose a single conceptual architecture capable of integrating the services and information-centric approaches for the future internet. We call this approach as Information and services. With reference to [4], Recent years have witnessed explosive growth in traffic demands combined with evolving content characteristics and dissemination patterns. This growth has resulted in an increasing demand for information identification as well as information-based communication functions that can meet this evolution. With reference to [5], The evolution towards emerging active distribution network can be realized via a real-time state estimation (RTSE) application facilitated by the use of phasor measurement units (PMUs). As such ,it aims to become a blueprint for the application of ICN-based general purpose communication platform to ADNs.From CP-ABE with centralized serverall attribute values and access policies are retrieved from the servers.This type of old scheme will not do ubiquitous distributed caching environment and completely relies on centralized servers.To solve this,we look up to a Distributed Publisher Driven(DPD) secure data sharing scheme to enable IoT data to be securely shared from the publishers to the user.

III. EXISTING SYSTEM

Flexible and fine-grained access control in cloud computing has been realized through Ciphertext Policy Attribute-Based Encryption (CPABE) with centralized server(s), wherein all attribute values and access policies are retrieved from the servers. In this paper, we denote these schemes as the existing CP-ABE scheme. The existing CP-ABE scheme does not consider a ubiquitous distributed caching environment and completely relies on centralized servers/clouds, which restricts the scalability.

IV. PROPOSED SYSTEM

We propose a Distributed Publisher driven secure Data sharing for ICIoT (DPD-ICIoT) to enable IoT data to be securely shared based on publisher defined policy. DPD-ICIoT provides flexible authorization from publishers to users. In DPD-ICIoT, CP-ABE is employed to provide flexible authorization from publishers to users.To balance centralized management and distributed retrievals for attributes, attribute manifest (AM) and data manifest (DM) are introduced and distributedly cached in the network.Thus, publishers can retrieve AMs from close copyholders instead of the centralized attribute servers. Herein, AM and DM are the data chunks, with the type of "Manifest", that describe attributes and data, respectively. Further, to reduce the large traffic overhead of attribute updates, we propose an

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Automatic Attribute Self-update Mechanism (AASM) to enable the update of attributes without querying the distant.It provide the correct data access to the users.It also provides attribute extraction service to the publisher,which means it assigns a start .In DPD-ICIoT,the basic building block of flexible data access authorization is introduced to provide the basic functions.The proposed DPD-ICIoT scheme can greatly reduce interaction times between Publishers and Users.If this DPD-ICIoT scheme help is not taken. The existing CP-ABE scheme does not consider a ubiquitous distributed caching environment and completely relies on centralized servers/clouds,with restricts the scalability of IoT system.

V. SYSTEM DESIGN

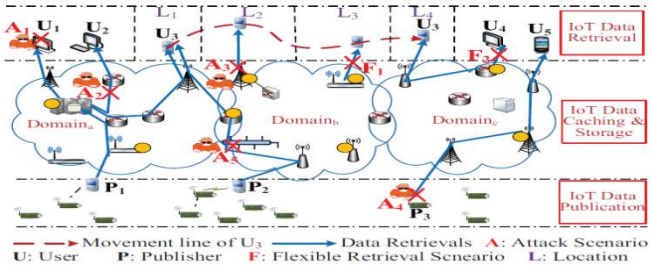

Fig.2 Architecture of Internet of Things

IoTs can be divided into three important layers that is;Perception,Network and Application as shown in the figure.6.a.[3]The Perception layer is also called as recognition layer which gathers the data or the information and recognises the physical world.Network layer being the middle layer (also called as wireless sensor networks) which does the initial processing of data,broadcasting of data,collection of data and combining it.The topmost layer is the Application layer which offers all these overhauls for all the industries.Among these three layers,the Network layer is the important layer and is also known as "Central Nervous System"[3]. It is called so because it takes care of all the global services in the IoTs,since it acts the part of aggregating with upward application layer and makes the link downward of perceptual layer. Various basic networks including wireless-wired network,mobile network offers the underlying connection.IoTs are set up in this new network which is composed Business applications of networks.

VI. IMPLEMENTATION

AES example-Input(128 bit key and message) key in English :Thats my Kung Fu(16 ASCII character, 1 byte each). Key in Hex(128 bits): 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75. Plaintext in English: Two one Nine two(16 ASCII character, 1 byte each).

The Advanced Encryption Standard all of the Cryptographic algorithm we have looked at so far have some problem. The earlier ciphers can be broken with ease on modern computation system. The DES algorithm was broken in 1998 using a system that cost about $250,000. It was also far too slow in software as it developed for mid-1970s hardware and does not produce efficient software code. Triple DES on the other hand ,has three times as many rounds as DES and is correspondingly slower .As well as this,the 64 bit block size of triples DES and DES is not efficient and is questionable when it comes to security.

There are five modules in the implementation they are, Publisher, User, DSA, DPD-ICIoT, Key generation. Publishers registers their IoT data attributes with the DSA and DSA issues the corresponding AMs to the network. AMs are cached in the network using the ICN approach. Users acquire permission to access a flexible set of IoT data from the DSA based on the attributes they hold. For Users, DSA generate private keys corresponding to their attributes. The Users and DSA authenticate each other based on the authentication service provided by NOA. DSA selects the bilinear group and master key, MK, and public key. DSA provides PK to Publisher and Users. Meanwhile it generate AMs and DMs according to the needs of Publishers, and then disseminates them in the network using the ICN approach.

RSA is one of the Public key cryptography methods. The RSA algorithm involves three steps: Key generation, encryption and decryption

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

- Step 1: if data is stolen in transit, the information can't be unscrambled without the private key's, which is based on the original prime numbers.
- Step 2: The usual attack on RSA involves factoring the large numbers which is the product of two very large prime numbers. The general idea behind this is the finding prime numbers is fairly easy.
- Step 3: The security of RSA itself is generally the least of our concerns in designing a system that uses it.
- Step 4: Encryption is general, it's even more consistently true with RSA than most other encryption.
- Step 5: A public key encryption technology developed by RSA data security, Inc. The acronym stands to Rivest, Shamir and Adelman security.

VII. EXPERIMENTAL RESULTS

We now provide some information on the performance achieved by the cpabe toolkit. Figure 3 displays measurements of private key generation time, encryption time, and decryption time produced by running cpabe-keygen,cpabe-enc, andcpabe-decon a rangeof problem sizes. The measurements were taken on a modern workstation.[4]The implementation uses a 160-bit elliptic curve group based on the supersingular curve $y^2 = x^3 + x$ over a 512-bit finite field. On the test machine, the PBC library can compute pairings in approximately 5.5ms, and exponentiations in G_0 and G_1 take about 6.4ms and 0.6ms respectively. Randomly selecting elements (by reading from the Linux kernel's /dev/random) is also a significant operation, requiringabout 16ms for G_0 and 1.6ms for G_1.As expected, cpabe-keygen runs in time precisely linear in the number of attributes associated with the key it is issuing. The running time of cpabe-enc is also almost perfectly linear with respect to the number of leaf nodes in the access policy. The polynomial operations at internal nodes amount to a modest number of multiplications and do not significantly contribute to the running time. Both remain quite feasible for even the largest problem instances.The performance of cpabe-dec is somewhat more interesting. It is slightly more difficult to measure in the absence of a precise application, since the decryption time can depend significantly on the particular access trees and set of attributes involved. In an at-tempt to average over this variation, we ran cpabe-dec on a series of ciphertexts that had been encrypted un-der randomly generated policy trees of various sizes. The trees were generated by starting with only a root node, then repeatedly adding a child to a randomly selected node until the desired number of leaf nodes was reached. At that point random thresholds were selected for each internal node. Since the time to decrypt also depends on the particular attributes available, for each run of cpabe-dec, we selected a key uniformly at random from all keys satisfying the policy. This was accomplished by iteratively taking random subsets of the attributes appearing in leaves of the tree and dis-carding those that did not satisfy it. A series of runs of cpabe-dec conducted in this manner produced the running times displayed.

These measurements give some insight into the effects of the optimizations described (all of which are implemented in the system). The line marked "naive" denotes the decryption time resulting from running the recursive DecryptNode algorithm and arbitrarily selecting nodes to satisfy each threshold gate. By ensuring that the final number of leaf nodes is minimized when making these decisions and replacing the DecryptNode algorithm with the "flattened" algorithm to reduce exponentiations, we obtain the im-proved times denoted "flatten". Perhaps most interestingly, employing the technique for merging pairings between leaf nodes sharing the same attribute, denoted "merge", actually increases running time in this case, due to fact that exponentiations are more expensive in G_0 than in G_1.

In summary, cpabe-keygen and cpabe-enc run in a predictable amount of time based on the number ofattributes in a key or leaves in a policy tree. The performance of cpabe-dec depends on the specific access tree of the ciphertext and the attributes available in the private key, and can be improved by some of the optimizations considered . In all cases, the toolkit consumes almost no overhead beyond the cost of the underlying group operations and random selection of elements. Large private keys and policies are possible in practice while maintaining reasonable running times.

VIII. CONCLUSION AND FUTURE ENHANCEMENT

The IoT technology brings about huge changes in everyone's everyday life. In the IoTs era, the short range mobile transceivers will be implanted in variety of daily requirements. The connections between communication of people and people will grow at any time in any location. The efficiency of information management and communications will arise to a new level. The environment of IoTs introduces unseen facilities for communication, which are going to change the

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

conceiving of computing and networking. The privacy and security implications of such an evolution should be carefully considered to the promising technology. The protection of data and privacy of users has been identified as one of the key challenges in the internet of things. In this survey, we presented internet of things with architecture and design goals. To march towards the secure IoT data sharing, we studied the IoT data sharing problem with respect to the unauthorised access, illegal modifications, and impersonation attack when IoT data are cached in the distributed manner throughout the network. We propose a novel DPD-ICIoT scheme for enabling secure and flexible access control for IoT data, which absorbs the merit from bothCP-ABE and CCN. The DPD-ICIoT scheme employs a keychain mechanism to provide efficient cryptographic operations. There are several issues to be addressed in realising secure IoT data sharing, such as trust management and IoT data life control. In the near future, we intend to integrate trust based relations into IoT data provision to advance the current research further.

We surveyed security and privacy concerns at different layers in IoTs. In addition, we identified several open issues related to the security and privacy that need to be addressed by research community to make secure and trusted platform for the delivery of future internet of things.

REFERENCES

[1] Sk. Md. M. Rahman,N.Nasser,and T. Taleb, "Pairing-based Secure Timing Synchronization for Heterogeneous Sensor Networks," *IEEE Globecom'08*, New Orleans, Louisiana,USA,Dec.2008.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute Based Encryption," *the 28thIEEE Symposium on Security and Privacy*, pp. 321- 334, Oakland, 2007

[3] J. Kumar, and D. Patel, "A Survey on Internet of Things: Security and Privacy Issues," *International Journal of Computer Applications*, vol. 90, no. 11, 2014.

[4] O.Vermesan and P.Friess (Editors), "Internet of Things:Converging Technologies for Smart Environments and Integrated Ecosystems," *River Publishers*,2013.

[5] D.Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything," *Cisco Internet Business Solutions Group white paper*,Apr,2011.

[6] W. chai, and et. al., "An Information-Centric Communication Infrastructure for Real-Time State Estimation of Active Distribution Networks," *IEEE Trans. On Smart Grid*, vol.6, no. 4,pp.2134-2146,July 2015